Art. 1 GDPRSubject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Art. 2 GDPRMaterial scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Regulation does not apply to the processing of personal data:
    1. in the course of an activity which falls outside the scope of Union law;
    2. by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
    3. by a natural person in the course of a purely personal or household activity;
    4. by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
3. [1]For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. [2]Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.
4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Art. 3 GDPRTerritorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
    1. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
    2. the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Art. 4 GDPRDefinitions

For the purposes of this Regulation:

1. ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2. ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3. ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

4. ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

5. ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

6. ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

7. ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

8. ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

9. [1]‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. [2]However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the

processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

10. ‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

11. ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

12. ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

13. ‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

14. ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

15. ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

16. ‘main establishment’ means:

    1. as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

    2. as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

17. ‘representative’ means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

18. ‘enterprise’ means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

19. ‘group of undertakings’ means a controlling undertaking and its controlled undertakings;

20. ‘binding corporate rules’ means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

21. ‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 51;

22. ‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because:

    1. the controller or processor is established on the territory of the Member State of that supervisory authority;

    2. data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

    3. a complaint has been lodged with that supervisory authority;

23. ‘cross-border processing’ means either:

    1. processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

    2. processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

24. ‘relevant and reasoned objection’ means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

25. ‘information society service’ means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council ([1]);

26. ‘international organisation’ means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Art. 5 GDPRPrinciples relating to processing of personal data

1. Personal data shall be:

    1. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Art. 6 GDPRLawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

    1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

    2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

    3. processing is necessary for compliance with a legal obligation to which the controller is subject;

    4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

    5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

    6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. [1]The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

    1. Union law; or

    2. Member State law to which the controller is subject.

[2]The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. [3]That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. [4]The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

    1. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

    2. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

    3. the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

    4. the possible consequences of the intended further processing for data subjects;

    5. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Art. 7 GDPRConditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. [1]If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. [2]Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. [1]The data subject shall have the right to withdraw his or her consent at any time. [2]The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. [3]Prior to giving consent, the data subject shall be informed thereof. [4]It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Art. 8 GDPRConditions applicable to child's consent in relation to information society services

1. [1]Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. [2]Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
[3]Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Art. 9 GDPRProcessing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

    1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

    2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

5. processing relates to personal data which are manifestly made public by the data subject;

6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Art. 10 GDPRProcessing of personal data relating to criminal convictions and offences

[1]Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. [2]Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Art. 11 GDPRProcessing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2. [1]Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. [2]In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

Art. 12 GDPRTransparent information, communication and modalities for the exercise of the rights of the data subject

1. [1]The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. [2]The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. [3]When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. [1]The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. [2]In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. [1]The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. [2]That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. [3]The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. [4]Where the data subject makes the request

by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. [1]Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. [2]Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

    1. charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

    2. refuse to act on the request.

[3]The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. [1]The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. [2]Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Art. 13 GDPRInformation to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

    1. the identity and the contact details of the controller and, where applicable, of the controller's representative;

    2. the contact details of the data protection officer, where applicable;

    3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

    4. where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

    5. the recipients or categories of recipients of the personal data, if any;

6. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

    1. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

    2. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

    3. where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

    4. the right to lodge a complaint with a supervisory authority;

    5. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

    6. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Suitable Recitals

Art. 14 GDPRInformation to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

    1. the identity and the contact details of the controller and, where applicable, of the controller's representative;

    2. the contact details of the data protection officer, where applicable;

3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4. the categories of personal data concerned;
5. the recipients or categories of recipients of the personal data, if any;
6. where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:
    1. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
    2. where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
    3. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
    4. where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
    5. the right to lodge a complaint with a supervisory authority;
    6. from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
    7. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:
    1. within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
    2. if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

3. if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

    1. the data subject already has the information;

    2. the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

    3. obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

    4. where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Art. 15 GDPRRight of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

    1. the purposes of the processing;

    2. the categories of personal data concerned;

    3. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

    4. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

    5. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

    6. the right to lodge a complaint with a supervisory authority;

    7. where the personal data are not collected from the data subject, any available information as to their source;

8. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. [1]The controller shall provide a copy of the personal data undergoing processing. [2]For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. [3]Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Art. 16 GDPRRight to rectification

[1]The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. [2]Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Art. 17 GDPRRight to erasure (‘right to be forgotten’)

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

    1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

    2. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

    3. the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

    4. the personal data have been unlawfully processed;

    5. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

    6. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology

and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
    1. for exercising the right of freedom of expression and information;
    2. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
    3. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
    4. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
    5. for the establishment, exercise or defence of legal claims.

Art. 18 GDPRRight to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
    1. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
    2. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
    3. the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
    4. the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.
2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.
3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Art. 19 GDPRNotification obligation regarding rectification or erasure of personal data or restriction of processing

[1]The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. [2]The controller shall inform the data subject about those recipients if the data subject requests it.

Art. 20 GDPRRight to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
    1. the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
    2. the processing is carried out by automated means.
2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
3. [1]The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. [2]That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Art. 21 GDPRRight to object

1. [1]The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. [2]The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for

such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Art. 22 GDPRAutomated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

    1. is necessary for entering into, or performance of, a contract between the data subject and a data controller;

    2. is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

    3. is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Art. 23 GDPRRestrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

1. national security;
2. defence;
3. public security;
4. the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
5. other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
6. the protection of judicial independence and judicial proceedings;
7. the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
8. a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
9. the protection of the data subject or the rights and freedoms of others;
10. the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:
    1. the purposes of the processing or categories of processing;
    2. the categories of personal data;
    3. the scope of the restrictions introduced;
    4. the safeguards to prevent abuse or unlawful access or transfer;
    5. the specification of the controller or categories of controllers;
    6. the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
    7. the risks to the rights and freedoms of data subjects; and
    8. the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

Art. 24 GDPRResponsibility of the controller

1. [1]Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. [2]Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Art. 25 GDPRData protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. [1]The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. [2]That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. [3]In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Art. 26 GDPRJoint controllers

1. [1]Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. [2]They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. [3]The arrangement may designate a contact point for data subjects.

2. [1]The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. [2]The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Art. 27 GDPRRepresentatives of controllers or processors not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. The obligation laid down in paragraph 1 of this Article shall not apply to:

    1. processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

    2. a public authority or body.

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Art. 28 GDPRProcessor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. [1]The processor shall not engage another processor without prior specific or general written authorisation of the controller. [2]In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. [1]Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. [2]That contract or other legal act shall stipulate, in particular, that the processor:

    1. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

    2. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

3. takes all measures required pursuant to Article 32;

4. respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

5. taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

6. assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

7. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

8. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. [1]Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. [2]Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Art. 29 GDPRProcessing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Art. 30 GDPRRecords of processing activities

1. [1]Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. [2]That record shall contain all of the following information:

    1. the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

    2. the purposes of the processing;

    3. a description of the categories of data subjects and of the categories of personal data;

    4. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

    5. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

    6. where possible, the envisaged time limits for erasure of the different categories of data;

    7. where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:
    1. the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
    2. the categories of processing carried out on behalf of each controller;
    3. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
    4. where possible, a general description of the technical and organisational security measures referred to in Article 32(1).
3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.
4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.
5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Art. 31 GDPRCooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Art. 32 GDPRSecurity of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
    1. the pseudonymisation and encryption of personal data;
    2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Art. 33 GDPRNotification of a personal data breach to the supervisory authority

1. [1]In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. [2]Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

    1. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    2. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

    3. describe the likely consequences of the personal data breach;

    4. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. [1]The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. [2]That documentation shall enable the supervisory authority to verify compliance with this Article.

Art. 34 GDPRCommunication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

    1. the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

    2. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

    3. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Art. 35 GDPRData protection impact assessment

1. [1]Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. [2]A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

    1. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

    2. processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

    3. a systematic monitoring of a publicly accessible area on a large scale.

4. [1]The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. [2]The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. [1]The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. [2]The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

    1. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

    2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

    3. an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

    4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Art. 36 GDPRPrior consultation

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. [1]Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. [2]That period may be extended by six weeks, taking into account the complexity of the intended processing. [3]The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. [4]Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

    1. where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

    2. the purposes and means of the intended processing;

    3. the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

    4. where applicable, the contact details of the data protection officer;

    5. the data protection impact assessment provided for in Article 35; and

    6. any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Art. 37 GDPRDesignation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

    1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

    2. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

3. the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. [1]In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. [2]The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Art. 38 GDPRPosition of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. [1]The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. [2]He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. [3]The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. [1]The data protection officer may fulfil other tasks and duties. [2]The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Art. 39 GDPRTasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

1. to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
2. to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
3. to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
4. to cooperate with the supervisory authority;
5. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing

Art. 40 GDPRCodes of conduct

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.
2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:
    1. fair and transparent processing;
    2. the legitimate interests pursued by controllers in specific contexts;
    3. the collection of personal data;
    4. the pseudonymisation of personal data;
    5. the information provided to the public and to data subjects;
    6. the exercise of the rights of data subjects;
    7. the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
    8. the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;
    9. the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

10. the transfer of personal data to third countries or international organisations; or

11. out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. [1]In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). [2]Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. [1]Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. [2]The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. [1]The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. [2]Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Art. 41 GDPRMonitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

    1. demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

    2. established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

    3. established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

    4. demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft requirements for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. [1]Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. [2]It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the requirements for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

Art. 42 GDPRCertification

1. [1]The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. [2]The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. [1]In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). [2]Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. [1]A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. [2]Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. [1]Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant criteria continue to be met. [2]Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the criteria for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Suitable Recitals

Art. 43 GDPRCertification bodies

1. [1]Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. [2]Member States shall ensure that those certification bodies are accredited by one or both of the following:

    1. the supervisory authority which is competent pursuant to Article 55 or 56;

    2. the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council[1] in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

    1. demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

    2. undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

    3. established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

    4. established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

    5. demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

3. [1]The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of requirements approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. [2]In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. [1]The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. [2]The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6. [1]The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. [2]The supervisory authorities shall also transmit those requirements and criteria to the Board.

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. [1]The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. [2]Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Art. 44 GDPRGeneral principle for transfers

[1]Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. [2]All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Suitable Recitals

Art. 45 GDPRTransfers on the basis of an adequacy decision

1. [1]A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. [2]Such a transfer shall not require any specific authorisation.
2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
    1. the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
    2. the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
    3. the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding

conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. [1]The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. [2]The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. [3]The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. [4]The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. [1]The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. [2]Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).
[3]On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Art. 46 GDPRTransfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or

processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:
    1. a legally binding and enforceable instrument between public authorities or bodies;
    2. binding corporate rules in accordance with Article 47;
    3. standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
    4. standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
    5. an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
    6. an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.
3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:
    1. contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
    2. provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.
4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.
5. [1]Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. [2]Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Art. 47 GDPRBinding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:
    1. are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;
    2. expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

3. fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

    1. the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

    2. the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

    3. their legally binding nature, both internally and externally;

    4. the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

    5. the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

    6. the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

    7. how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

    8. the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

    9. the complaint procedures;

    10. the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

11. the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

12. the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

13. the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

14. the appropriate data protection training to personnel having permanent or regular access to personal data.

3. [1]The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. [2]Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Art. 48 GDPR Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Art. 49 GDPRDerogations for specific situations

1. [1]In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

    1. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

    2. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

3. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

4. the transfer is necessary for important reasons of public interest;

5. the transfer is necessary for the establishment, exercise or defence of legal claims;

6. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

7. the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

[2]Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. [3]The controller shall inform the supervisory authority of the transfer. [4]The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. [1]A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. [2]Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. [1]In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. [2]Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Art. 50 GDPRInternational cooperation for the protection of personal data

1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:
    1. develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
    2. provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
    3. engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;
    4. promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

Art. 51 GDPRSupervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

2. [1]Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. [2]For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Art. 52 GDPRIndependence

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Suitable Recitals

(117) Establishment of Supervisory Authorities (118) Monitoring of the Supervisory Authorities (120) Features of Supervisory Authorities (121) Independence of the Supervisory Authorities

Art. 53 GDPRGeneral conditions for the members of the supervisory authority

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:
   – their parliament;
   – their government;
   – their head of State; or
   – an independent body entrusted with the appointment under Member State law.

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Art. 54 GDPRRules on the establishment of the supervisory authority

1. Each Member State shall provide by law for all of the following:

    1. the establishment of each supervisory authority;

    2. the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;

    3. the rules and procedures for the appointment of the member or members of each supervisory authority;

    4. the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

    5. whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;

    6. the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. [1]The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. [2]During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

Art. 55 GDPRCompetence

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. [1]Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. [2]In such cases Article 56 does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Art. 56 GDPRCompetence of the lead supervisory authority

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

3. [1]In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. [2]Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. [1]Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. [2]The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. [3]The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Art. 57 GDPRTasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

    1. monitor and enforce the application of this Regulation;

    2. promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

    3. advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

4. promote the awareness of controllers and processors of their obligations under this Regulation;

5. upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

6. handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

7. cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

8. conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

9. monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

10. adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

11. establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

12. give advice on the processing operations referred to in Article 36(2);

13. encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

14. encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

15. where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

16. draft and publish the requirements for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

17. conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

18. authorise contractual clauses and provisions referred to in Article 46(3);

19. approve binding corporate rules pursuant to Article 47;

20. contribute to the activities of the Board;

21. keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

22. fulfil any other tasks related to the protection of personal data.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

4. [1]Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. [2]The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Art. 58 GDPRPowers

1. Each supervisory authority shall have all of the following investigative powers:

    1. to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

    2. to carry out investigations in the form of data protection audits;

    3. to carry out a review on certifications issued pursuant to Article 42(7);

    4. to notify the controller or the processor of an alleged infringement of this Regulation;

    5. to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

    6. to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

    1. to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

    2. to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

    3. to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

    4. to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

    5. to order the controller to communicate a personal data breach to the data subject;

6. to impose a temporary or definitive limitation including a ban on processing;

7. to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

8. to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

9. to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

10. to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

    1. to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

    2. to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

    3. to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

    4. to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

    5. to accredit certification bodies pursuant to Article 43

    6. to issue certifications and approve criteria of certification in accordance with Article 42(5);

    7. to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

    8. to authorise contractual clauses referred to in point (a) of Article 46(3);

    9. to authorise administrative arrangements referred to in point (b) of Article 46(3);

    10. to approve binding corporate rules pursuant to Article 47.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and

where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

6. [1]Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. [2]The exercise of those powers shall not impair the effective operation of Chapter VII.

Art. 59 GDPRActivity reports

[1]Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). [2]Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. [3]They shall be made available to the public, to the Commission and to the Board

Art. 60 GDPRCooperation between the lead supervisory authority and the other supervisory authorities concerned

1. [1]The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. [2]The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. [1]The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. [2]It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.

5. [1]Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. [2]That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

7. [1]The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. [2]The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

9. [1]Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. [2]The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

10. [1]After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. [2]The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

Art. 61 GDPRMutual assistance

1. [1]Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. [2]Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. [1]Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. [2]Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. [1]Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. [2]Information exchanged shall be used only for the purpose for which it was requested.

4. The requested supervisory authority shall not refuse to comply with the request unless:

    1. it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

    2. compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

5. [1]The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. [2]The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. [1]Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. [2]Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. [1]Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). [2]In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

9. [1]The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. [2]Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Art. 62 GDPRJoint operations of supervisory authorities

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.

2. [1]Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. [2]The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.

3. [1]A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the

seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. [2]Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. [3]The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.

4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

5. [1]The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. [2]The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.

6. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.

7. [1]Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. [2]In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

Art. 63 GDPRConsistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

Art. 64 GDPROpinion of the Board

1. [1]The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. [2]To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

    1. aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);

    2. concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;

3. aims to approve the requirements for accreditation of a body pursuant to Article 41(3), of a certification body pursuant to Article 43(3) or the criteria for certification referred to in Article 42(5);

4. aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and in Article 28(8);

5. aims to authorise contractual clauses referred to in point (a) of Article 46(3); or

6. aims to approve binding corporate rules within the meaning of Article 47.

2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

3. [1]In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. [2]That opinion shall be adopted within eight weeks by simple majority of the members of the Board. [3]That period may be extended by a further six weeks, taking into account the complexity of the subject matter. [4]Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

5. The Chair of the Board shall, without undue, delay inform by electronic means:

    1. the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and

    2. the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

6. The competent supervisory authority referred to in paragraph 1 shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.

7. The competent supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.

8. Where the competent supervisory authority referred to in paragraph 1 informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend

to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

Art. 65 GDPRDispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

    1. where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead supervisory authority and the lead supervisory authority has not followed the objection or has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

    2. where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

    3. where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

2. [1]The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. [2]That period may be extended by a further month on account of the complexity of the subject-matter. [3]The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

3. [1]Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. [2]Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. [1]The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. [2]It shall inform the Commission thereof. [3]The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. [1]The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. [2]The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. [3]The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). [4]The final decision

shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. [5]The final decision shall attach the decision referred to in paragraph 1 of this Article.

Art. 66 GDPRUrgency procedure

1. [1]In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. [2]The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

Art. 67 GDPRExchange of information

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Art. 68 GDPREuropean Data Protection Board

1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.

2. The Board shall be represented by its Chair.

3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.

5. [1]The Commission shall have the right to participate in the activities and meetings of the Board without voting right. [2]The Commission shall designate a representative. [3]The Chair of the Board shall communicate to the Commission the activities of the Board.

6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

Art. 69 GDPRIndependence

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.

2. Without prejudice to requests by the Commission referred to in Article 70(1) and (2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

Art. 70 GDPRTasks of the Board

1. [1]The Board shall ensure the consistent application of this Regulation. [2]To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:

    1. monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;

    2. advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

    3. advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;

    4. issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);

    5. examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;

    6. issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);

    7. issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

    8. issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to

result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).

9. issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;

10. issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);

11. draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;

12. review the practical application of the guidelines, recommendations and best practices;

13. issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);

14. encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;

15. approve the criteria of certification pursuant to Article 42(5) and maintain a public register of certification mechanisms and data protection seals and marks pursuant to Article 42(8) and of the certified controllers or processors established in third countries pursuant to Article 42(7);

16. approve the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies referred to in Article 43;

17. provide the Commission with an opinion on the certification requirements referred to in Article 43(8);

18. provide the Commission with an opinion on the icons referred to in Article 12(7);

19. provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

20. issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant

to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;

21. promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

22. promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

23. promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

24. issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and

25. maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

4. [1]The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. [2]The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

rt. 71 GDPRReports

1. [1]The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. [2]The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.

2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

Art. 72 GDPRProcedure

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.

Art. 73 GDPRChair

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.

2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

Art. 74 GDPRTasks of the Chair

1. The Chair shall have the following tasks:
    1. to convene the meetings of the Board and prepare its agenda;
    2. to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;
    3. to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.
2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

Art. 75 GDPRSecretariat

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.
2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.
3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.
4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.
5. The secretariat shall provide analytical, administrative and logistical support to the Board.
6. The secretariat shall be responsible in particular for:
    1. the day-to-day business of the Board;
    2. communication between the members of the Board, its Chair and the Commission;
    3. communication with other institutions and the public;
    4. the use of electronic means for the internal and external communication;
    5. the translation of relevant information;
    6. the preparation and follow-up of the meetings of the Board;
    7. the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

Art. 76 GDPRConfidentiality

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council[1].

Art. 77 GDPRRight to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Art. 78 GDPRRight to an effective judicial remedy against a supervisory authority

Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Art. 79 GDPRRight to an effective judicial remedy against a controller or processor

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

1Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. 2Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Art. 80 GDPRRepresentation of data subjects

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their

personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

Art. 81 GDPRSuspension of proceedings

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof

Art. 82 GDPRRight to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. [1]Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. [2]A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the

compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Art. 83 GDPRGeneral conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. [1]Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). [2]When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

    1. the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

    2. the intentional or negligent character of the infringement;

    3. any action taken by the controller or processor to mitigate the damage suffered by data subjects;

    4. the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

    5. any relevant previous infringements by the controller or processor;

    6. the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

    7. the categories of personal data affected by the infringement;

    8. the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

    9. where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

    10. adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

    11. any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

    1. the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

    2. the obligations of the certification body pursuant to Articles 42 and 43;

    3. the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

    1. the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

    2. the data subjects' rights pursuant to Articles 12 to 22;

    3. the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

    4. any obligations pursuant to Member State law adopted under Chapter IX;

    5. non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. [1]Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. [2]In any event, the fines imposed shall be effective, proportionate and dissuasive. [3]Those Member States shall notify to the Commission the

provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

Suitable Recitals

Art. 84 GDPRPenalties

1. [1]Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. [2]Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Art. 85 GDPRProcessing and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Art. 86 GDPRProcessing and public access to official documents

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Art. 87 GDPRProcessing of the national identification number

[1]Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. [2]In that case the national

identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Art. 88 GDPRProcessing in the context of employment

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Art. 89 GDPRSafeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. [1]Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. [2]Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. [3]Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. [4]Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Art. 90 GDPRObligations of secrecy

1. [1]Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. [2]Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Art. 91 GDPRExisting data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

Art. 92 GDPRExercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.

3. [1]The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. [2]A decision of revocation shall put an end to the delegation of power specified in that decision. [3]It shall take effect the day following that of its publication in the *Official Journal of the European Unio*n or at a later date specified therein. [4]It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. [1]A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. [2]That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Art. 93 GDPRCommittee procedure

1. [1]The Commission shall be assisted by a committee. [2]That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
3. Where reference is made to this paragraph, Article 8 of Regulation ((EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

Art. 94 GDPRRepeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed with effect from 25 May 2018.
2. [1]References to the repealed Directive shall be construed as references to this Regulation. [2]References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Art. 95 GDPRRelationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

Art. 96 GDPRRelationship with previously concluded Agreements

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

Art. 97 GDPRCommission reports

1. [1]By 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. [2]The reports shall be made public.
2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:
    1. Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;
    2. Chapter VII on cooperation and consistency.

3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.
4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.
5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

Art. 98 GDPRReview of other Union legal acts on data protection

[1]The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. [2]This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

Art. 99 GDPREntry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.
2. It shall apply from 25 May 2018.

Carnegie Mellon
INFORMATION SECURITY OFFICE

Computer Security Incident Response Plan

Name of Approver: Mary Ann Blair	Effective Date: 23-FEB-2014
Date of Approval: 23-FEB-2014	
Date of Review: 26-APR-2023	Name of Reviewer: Laura Raderman/John Lerchey

Carnegie Mellon
INFORMATION SECURITY OFFICE

Table of Contents

Introduction

Purpose

This document describes the overall plan for responding to information security incidents at Carnegie Mellon University. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The goal of the Computer Security Incident Response Plan is to provide a framework to ensure that potential computer security incidents are managed in an effective and consistent manner. This includes evaluation to determine scope and potential risk, appropriate response, clear communication to stakeholders, containment, remediation and restoration of service, and plans for reducing the chance of recurrence.

Scope

This plan applies to the Information Systems, Institutional Data, and networks of Carnegie Mellon University and any person or device who gains access to these systems or data.

Maintenance

The University's Information Security Office (ISO) is responsible for the maintenance and revision of this document.

Authority

The ISO is charged with executing this plan by virtue of its original charter and various policies such as the Computing Policy, Information Security Policy, and HIPAA Policy.

Relationship to other Policies

This plan incorporates the risk profiles for Institutional Data as outlined in the Guidelines for Data Classification.

Relationship to Other Groups at CMU

The ISO acts on behalf of the University community and will ask for cooperation and assistance from community members as required. The ISO also works closely with University administrative groups such as the Student Life Office, Human Resources, and the Office of General Counsel in investigations and e-discovery matters, and at their behest may assist Law Enforcement.

Definitions

Event

An event is an exception to the normal operation of IT infrastructure, systems, or services. Not all events become incidents.

Incident

An incident is an event that, as assessed by ISO staff, violates the Computing Policy; Information Security Policy; other University policy, standard, or code of conduct; or

threatens the confidentiality, integrity, or availability of Information Systems or Institutional Data.

Incidents may be established by review of a variety of sources including, but not limited to ISO monitoring systems, reports from CMU staff or outside organizations and service degradations or outages. Discovered incidents will be declared and documented in ISO's incident documentation system.

Complete IT service outages may also be caused by security-related incidents, but service outage procedures will be detailed in Business Continuity and/or Disaster Recovery procedures.

Incidents will be categorized according to the potential for restricted data exposure, the criticality of a resource, scope, and the potential for persistence using a High-Medium-Low designation. The initial severity may be adjusted during plan execution.

Detected vulnerabilities will not be classified as incidents. The ISO employs tools to scan the CMU environment and depending on severity of found vulnerabilities may warn affected users, disconnect affected machines, or apply other mitigations. In the absence of indications of compromise or sensitive data exposure, vulnerabilities will be communicated and the ISO will pursue available technology remedies to reduce risk.

Data Classification

Incident response processes take into account data classification when determining the categorization of an incident and relevant communications. Data classifications are found at: https://www.cmu.edu/iso/governance/guidelines/data-classification.html

Roles and Responsibilities

The Incident Response Process incorporates the Information Security Roles and Responsibilities definitions and extends or adds the following Roles.

Incident Response Coordinator

The Incident Response Coordinator is the ISO employee who is responsible for assembling all the data pertinent to an incident, communicating with appropriate parties, ensuring that the information is complete, and reporting on incident status both during and after the investigation.

Incident Response Handlers

Incident Response Handlers are employees of the ISO, other CMU staff, or outside contractors who gather, preserve and analyze evidence so that an incident can be brought to a conclusion.

Insider Threats
Insiders are, according to CERT[1], current or former employees, contractors, or business partners who have access to an organization's restricted data and may use their access to threaten the confidentiality, integrity or availability of an organization's information or systems. This particular threat is defined because it requires special organizational and technical amendments to the Incident Response Plan as detailed below.

Law Enforcement
Law Enforcement includes the CMU Police, federal, state and local law enforcement agencies, and U.S. government agencies that present warrants or subpoenas for the disclosure of information. Interactions with these groups will be coordinated with the Office of General Counsel (see below).

Office of General Counsel (OGC)
The University's Office of General Counsel (OGC) acts as the liaison between the ISO and external Law Enforcement, and provides guidance on the extent and form of all responses and disclosures to law enforcement and the public.

Officers
Officers are the staff designates for various regulatory frameworks to which the University is required to comply.

Key Stakeholders
Key Stakeholders are those individuals that have decision-making authority for their areas of responsibility.

Users
Users are members of the CMU community or anyone accessing an Information System, Institutional Data or CMU networks who may be affected by an incident.

Methodology
This plan outlines the most general tasks for Incident Response and will be supplemented by specific internal guidelines and procedures that describe the use of security tools and/or channels of communication. These internal guidelines and procedures are subject to amendment as technology changes. These guidelines will be documented in detail and kept up-to-date.

Constituencies
The ISO represents the entire University's Information System(s) and Institutional Data, supporting the Users. Some departments and schools maintain their own IT staffs and some branches of the university are located in other cities or countries. To the extent

[1] This is a paraphrase of the definition presented in the Software Engineering Institute's 2009 publication entitled "Common Sense Guide to Prevention and Detection of Insider Threats" (Capelli et al, third edition, v3.1)

possible, the ISO will attempt to coordinate its efforts with these other groups and to represent the University's security posture and activities. Specific actions to be taken will be determined by the type, scope, and risk of the threat. For example, more resources may be applied to a potential disclosure of PII or ePHI than would be applied to a single ad-ware infection.

Evidence Preservation

The goal of Incident Response is to reduce and contain the scope of an incident and ensure that IT assets are returned to service as quickly as possible. Rapid response is balanced by the requirement to collect and preserve evidence in a manner consistent with the requirements of rules 26-34 of the Federal Rules of Civil Discovery, and to abide by legal and Administrative requirements for documentation and chain of custody. ISO will maintain and disseminate procedures to clarify specific activities in the ISO and in CMU departments with regard to evidence preservation, and will adjust those procedures as technologies change.

Operational-Level Agreements, Governance

Computing groups have operational-level agreements with the customers they serve. Interruption of service is a hardship and the ISO will cooperate with these groups to ensure that downtime is minimized. However, the ISO's management supports the priority of investigation activities where there is significant risk, and this may result in temporary outages or interruptions.

Staffing for an Incident Response Capability, Resiliency

The ISO will endeavor to maintain sufficient staffing and third-party augmentation to investigate each incident to completion and communicate its status to other parties while it monitors the tools that detect new events. Insufficient staffing will impact rapid response capability and resiliency, as will degradation of the tools used for detection, monitoring, and response.

Training

The continuous improvement of incident handling processes implies that those processes are periodically reviewed, tested and translated into recommendations for enhancements. CMU staff inside and outside of the ISO will be periodically trained on procedures for reporting and handling incidents to ensure that there is a consistent and appropriate response to incidents, and that post-incident findings are incorporated into procedural enhancements.

Incident Response Phases

The basic incident process encompasses six phases: preparation, detection, containment, investigation, remediation and recovery. The dynamic relationship between those phases is highlighted in Figure 1. These phases are defined in NIST SP 800-61 (Computer Security Incident Handling Guide). The ISO's overall incident response process includes detection, containment, investigation, remediation and recovery, documented in specific procedures

it maintains. This plan is the primary guide to the preparation phase from a governance perspective; local guidelines and procedures will allow the ISO to be ready to respond to any incident. Recovery includes re-evaluating whether the preparation or specific procedures used in each phase are appropriate and modifying them if inappropriate.

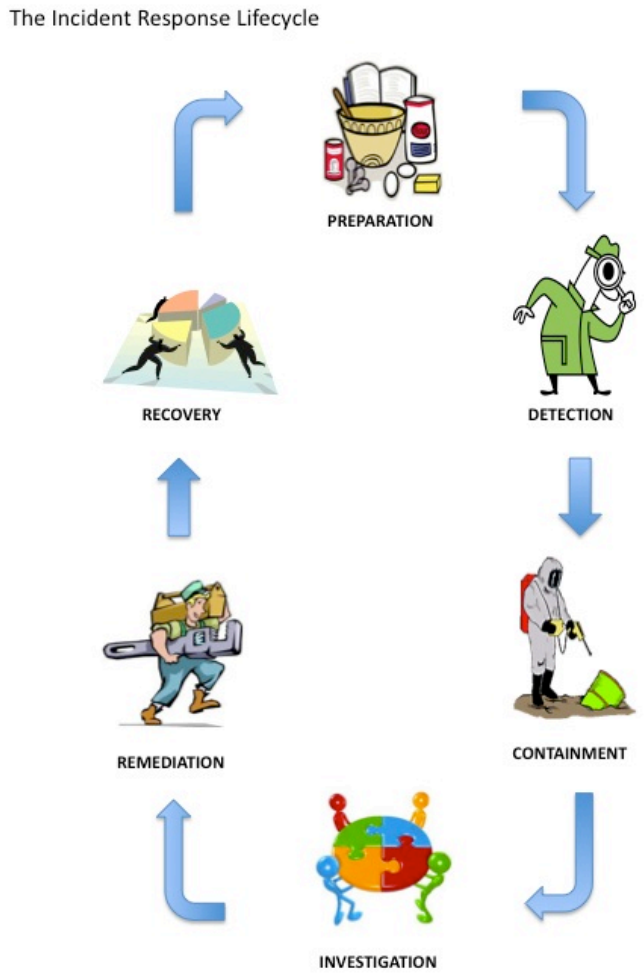

Figure 1

Preparation

Preparation includes those activities that enable the ISO to respond to an incident: policies, tools, procedures, effective governance and communication plans. Preparation also implies that the affected groups have instituted the controls necessary to recover and continue operations after an incident is discovered. Post-mortem analyses from prior incidents should form the basis for continuous improvement of this stage.

Detection
Detection is the discovery of the event with security tools or notification by an inside or outside party about a suspected incident. This phase includes the declaration and initial classification of the incident, as well as any initial notifications required by law or contract.

Containment
Containment is the triage phase where the affected host or system is identified, isolated or otherwise mitigated, and when affected parties are notified and investigative status established. This phase includes sub-procedures for seizure and evidence handling, escalation, and communication.

Investigation
Investigation is the phase where ISO personnel determine the priority, scope, risk, and root cause of the incident.

Remediation
Remediation is the post-incident repair of affected systems, communication and instruction to affected parties, and analysis that confirms the threat has been remediated. Any determination of regulatory requirements and all internal and external communications are determined by Key Stakeholders. Apart from any formal reports, the post-mortem will be completed at this stage as it may impact the remediation and interpretation of the incident.

Recovery
Recovery is the analysis of the incident for its procedural and policy implications, the gathering of metrics, and the incorporation of "lessons learned" into future response activities and training.

Specific procedures related to this Incident response plan are documented at the ISO's Policies and Procedures internal site.

Guidelines for the Incident Response Process
In the process of responding to an incident, many questions arise and problems are encountered, any of which may be different for each incident. This section provides guidelines for addressing common issues. The Incident Response Coordinator, Director of Information Security, Chief Information Security Officer and Office of General Counsel should be consulted for questions and incident types not covered by these guidelines.

Insider Threats
In the case that a particular Incident Response Handler is a person of interest in an incident, the Incident Response Coordinator will assign other Incident Response Handlers to the incident.

In the case that the Incident Response Coordinator is a person of interest in an incident, the Chief Information Security Officer will act in their stead or appoint a designee to act on their behalf.

In the case that the Chief Information Security Officer is a person of interest in an incident, the Chief Information Officer (CIO) will act in their stead or appoint a designee to act on their behalf.

In the case that another CMU administrative authority is a person of interest in an incident, the ISO will work with the remaining administrative authorities in the ISO's reporting line to designate a particular point of contact or protocol for communications.

Interactions with Law Enforcement

All communications with external law enforcement authorities are made after consulting with the Office of General Counsel. The ISO works with CMU Police, where authorized by OGC, to determine their information requirements and shares the minimum necessary information as required for incident response.

Communications Plan

All public communications about an incident or incident response to external parties outside of CMU are made in consultation with OGC and Media Relations. Private or internal communications with other affected or interested parties contain the minimum information necessary. The minimum information necessary to share for a particular incident is determined by the Incident Response Coordinator and the Chief Information Security Officer in consultation with OGC or other campus administrative authorities.

Privacy

The Computing Policy provides specific requirements for maintaining the privacy of University affiliates. All incident response procedures will follow the current privacy requirements as set out in the Computing Policy. Exceptions must be approved by OGC.

Documentation, Tracking and Reporting

All incident response activities will be documented to include artifacts obtained using methods consistent with chain of custody and confidentiality requirements. Documentation is sufficient to support the declaration, remediation, and recovery from the incident. Incidents will be prioritized and ranked according to their potential risk. As an investigation progresses, that ranking may change, resulting in a greater or lesser prioritization of ISO resources.

Incidents will be reviewed post-mortem to assess whether the investigational process was successful and effective. Subsequent adjustments may be made to methods and procedures used by the ISO and by other participants to improve the incident response process.

Artifacts obtained during the course of an investigation may be deleted after the conclusion of the investigation and post-mortem analysis unless otherwise directed by OGC.

Escalation

At any time during the incident response process, the Incident Response Coordinator, Director of Information Security and the Chief Information Security Officer may be called upon to escalate any issue regarding the process or incident.

The Incident Response Coordinator and Chief Information Security Officer in consultation with OGC will determine if and when an incident should be escalated to external authorities.

Further Information

Further information on the Computer Security Incident Response Plan and associated procedures can be obtained from the Incident Response Coordinator of the ISO via iso-ir@andrew.cmu.edu or 412-268-2044.

Revision History

Version	Date	Author	Description
1.0	13-FEB-2014	Laura Raderman <lbowser>	Initial Document
1.1	31-MAY-2016	Laura Raderman <lbowser>	Added "local" to the definition of law enforcement, and changed link to NIST SP 800-61
1.2	24-MAR-2017	John Lerchey <lerchey>	Minor edits.
1.3	31-MAY-2017	Laura Raderman <lbowser>	Updated links.
1.4	06-JUN-2019	John Lerchey <lerchey>	Reviews and minor detail updates. Added GDPR PII definitions.
1.5	08-SEP-2020	Laura Raderman <lbowser>	Minor edits
1.6	10-FEB-2022	Laura Raderman <lbowser>	Removed section of data types and reference Guidelines for Data Classification, minor updates for 2021 GLBA Safeguards Rule

National Security Agency
Cybersecurity Technical Report

Network Infrastructure Security Guide

October 2023

U/OO/118623-22
PP-22-0293
Version 1.2

Notices and history

Document change history

Date	Version	Description
October 2023	1.2	Updated links to references
June 2022	1.1	Minor clarifications and additional vendor links
March 2022	1.0	Report released

Disclaimer of warranties and endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guide shall not be used for advertising or product endorsement purposes.

Trademark recognition

Cisco® and Cisco IOS® are registered trademarks of Cisco Systems, Inc.

Publication information

Author(s)

National Security Agency
Cybersecurity Directorate

Contact information

Client Requirements / General Cybersecurity Inquiries:
Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov

Media inquiries / Press Desk:
Media Relations, 443-634-0721, MediaRelations@nsa.gov

Defense Industrial Base Inquiries for Cybersecurity Services:
DIB Cybersecurity Program, DIB_Defense@cyber.nsa.gov

Purpose

This document was developed in furtherance of NSA's cybersecurity missions. This includes its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense information systems, and the Defense Industrial Base, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contents

1. Introduction

Guidance for securing networks continues to evolve as adversaries exploit new vulnerabilities, new security features are implemented, and new methods of securing devices are identified. Improper configurations, incorrect handling of configurations, and weak encryption keys can expose vulnerabilities in the entire network. All networks are at risk of compromise, especially if devices are not properly configured and maintained. An administrator's role is critical to securing the network against adversarial techniques and requires dedicated people to secure the devices, applications, and information on the network.

An administrator's role is critical in securing networks.

This report presents best practices for overall network security and protection of individual network devices. It will assist administrators in preventing an adversary from exploiting their network. While the guidance presented here can be applied to many types of network devices, the National Security Agency (NSA) has provided sample commands for Cisco Internetwork Operating System (IOS) devices. These commands can be executed to implement recommended mitigations.

1.1 Regarding Zero Trust

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. NSA fully supports the Zero Trust security model, and much of the guidance in this report can be applied at different boundaries as recommended in Zero Trust guidance. However, this report provides guidance to mitigate common vulnerabilities and weaknesses on existing networks. As system owners introduce new network designs intended to achieve more mature Zero Trust principles, this guide may need to be modified.

2. Network architecture and design

A secure network design that implements multiple defensive layers is critical to defend against threats and protect resources within the network. The design should follow security best practices and model Zero Trust principles, both for network perimeter and internal devices.

Apply multiple layers of defense for a more secure network design.

2.1 Install perimeter and internal defense devices

A network requires a substantial defensive strategy to protect individual components and the information they contain. Multiple layers of defense should be implemented at the network's perimeter to protect against external threats, and to monitor and restrict inbound and outbound traffic.

NSA recommends configuring and installing security devices at the perimeter of the network according to security best practices:

- Install a border router to facilitate a connection to the external network, such as an Internet service provider (ISP).
- Implement multiple layers of next-generation firewalls throughout the network to restrict inbound traffic, restrict outbound traffic, and examine all internal activity between disparate network regions. Each layer should utilize different vendors to protect against an adversary exploiting the same unpatched vulnerability in an attempt to access the internal network.
- Place publicly accessible systems and outbound proxies in between the firewall layers in one or more demilitarized zone (DMZ) subnets, where access can be appropriately controlled between external devices, DMZ devices, and internal systems.
- Implement a network monitoring solution to log and track inbound and outbound traffic, such as a network intrusion detection system (NIDS), a traffic inspector, or a full-packet capture device.
- Deploy multiple dedicated remote log servers to enable activity correlation among devices and detection of lateral movement.
- Implement redundant devices in core areas to ensure availability, which can be load-balanced to increase network throughput and decrease latency.

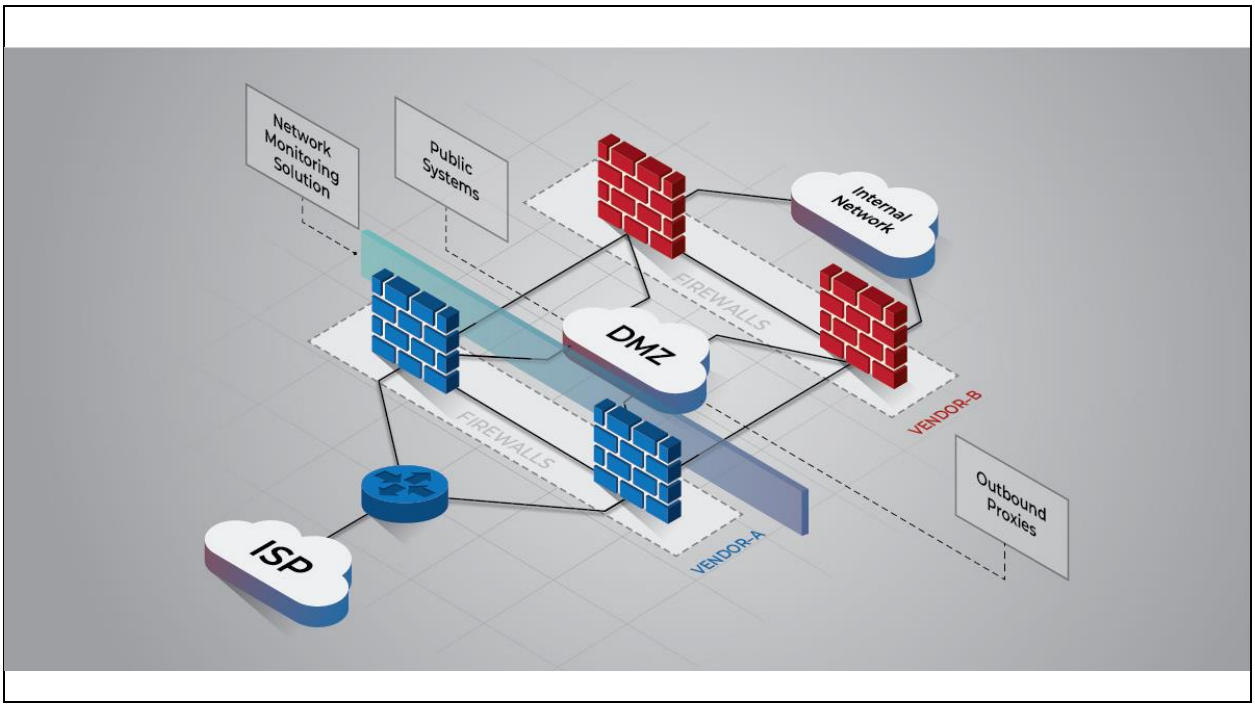

Figure 1: Network perimeter with firewalls and a DMZ

2.2 Group similar network systems

Similar systems within a network should be logically grouped together to protect against adversarial lateral movement from other types of systems. Adversaries will target systems that are easier to exploit, such as printers, and use that initial access to further propagate to other systems on the network. Proper network segmentation significantly reduces the ability for an adversary to reach and exploit these other systems (see Cybersecurity and Infrastructure Security Agency's (CISA's) "Layering Network Security Through Segmentation" and NSA's "Segment Networks and Deploy Application-aware Defenses") [1], [2]. Additionally, access restrictions between different types of systems are easier to manage, control, and monitor if they are logically grouped together.

NSA recommends isolating similar systems into different subnets or virtual local area networks (VLANs), or physically separating the different subnets via firewalls or filtering routers. Workstations, servers, printers, telecommunication systems, and other network peripherals should be separate from each other. Operational technology, such as industrial control systems, typically need to be isolated from other information technology and high-risk networks like the Internet. This physical separation provides stronger protection because the intermediate device between subnets must be compromised for an adversary to bypass access restrictions. Implement access

restrictions on the internal routers, switches, or firewalls to allow only those ports and protocols that are required for network operations or valid mission need. Access control lists (ACLs) may need to be duplicated and applied directly to the switches to restrict access between VLANs, or they can be applied to core routers where routing is performed between internal subnets.

2.3 Remove backdoor connections

A backdoor network connection is between two or more devices located in different network areas, generally with different types of data and security requirements. If one device is compromised, an adversary can use this connection to bypass access restrictions and gain access to other areas of the network. An example of a backdoor network connection is an external border router connected to an ISP that is also directly connected to the internal or management subnets. An adversary that can compromise this external border router would likely have access to the internal network, bypassing all firewalls.

NSA recommends removing all backdoor network connections and using caution when connecting devices with more than one network interface. Verify that all network interfaces of a device are at similar security levels, or that an intermediate device provides both logical and physical separation between different network areas.

2.4 Utilize strict perimeter access controls

Network perimeter devices are essential elements in a security model and should be configured to complement each other by implementing ACLs to regulate ingress and egress of network traffic. These access control rulesets should be configured to explicitly allow only services and systems that are required to support the mission of the network.

NSA recommends a deny-by-default, permit-by-exception approach achieved by carefully considering which connections to allow, and then creating rulesets that focus on permitting only the allowed connections. This method allows a single rule to deny several types of connections, instead of needing to create a separate rule for each blocked connection. Failure to use a deny-by-default, permit-by-exception approach can permit unnecessary access and increase the risk of compromise and information gathering. If it is necessary to dynamically apply additional perimeter rulesets to prevent

an adversary from completing or continuing an exploit, NSA recommends the use of an intrusion prevention system (IPS).

NSA also recommends enabling logging, at a minimum, on all rulesets that deny or drop network traffic. Logging should also be enabled on successful **and** unsuccessful administrator access to critical devices.

2.5 Implement a network access control (NAC) solution

An adversary who wishes to gain internal access to a network must either find a way through the external perimeter of the network or obtain access from inside the network. A NAC solution prevents unauthorized physical connections and monitors authorized physical connections on a network.

NSA recommends implementing a NAC solution that identifies and authenticates unique devices connected to the network. Port security is a mechanism that can be implemented on switches to detect when unauthorized devices are connected to the network via a device's media access control (MAC) address.

However, port security can be difficult to manage. For example, it increases the number of support tickets due to valid blocked network ports (e.g., connected devices that change often, such as conference rooms). In addition, adversaries who can spoof a MAC address can bypass it as well. A more robust solution utilizes 802.1X, which authenticates devices based on a trusted digital certificate installed on the device. While it is more complex to implement, due to the use of certificates, it is easier to manage than port security and offers a higher level of assurance.

2.6 Limit virtual private networks (VPNs)

A VPN tunnel can be established between two endpoints to provide an encrypted communication channel over a network. It should only be used when the confidentiality and integrity of the traffic cannot be maintained through other methods. VPN gateways are typically accessible from the Internet and are prone to network scanning, brute force attempts, and zero-day vulnerabilities. To mitigate many of these vulnerabilities, disable all unnecessary features on the VPN gateways and implement strict traffic filtering rules [2].

NSA recommends limiting VPN gateway access to User Datagram Protocol (UDP) port 500, UDP port 4500, Encapsulating Security Payload (ESP), and other appropriate

ports as needed. When possible, limit accepted traffic to known VPN peer Internet Protocol (IP) addresses. Remote access VPNs cannot be added to a static filtering rule if the remote peer IP address is unknown. If traffic cannot be filtered to specific IP addresses, use an IPS in front of the VPN gateway to monitor for malformed IP Security (IPsec) traffic and inspect IPsec session negotiations [3].

All IPsec VPN configurations require an IPsec policy and an Internet Key Exchange (IKE) policy. These policies determine how it will negotiate each phase when establishing the IPsec tunnel. If either phase is configured to allow weak cryptography, the entire VPN may be at risk and data confidentiality will be lost. Each IKE policy includes at least three key components:

1. Diffie-Hellman algorithm/group
2. Encryption algorithm
3. Hashing algorithm

The following are the minimum recommended settings per Committee on National Security Systems Policy (CNSSP) 15:

- Diffie-Hellman Group: 16 with 4096 bit Modular Exponent (MODP)
- Diffie-Hellman Group: 20 with 384 bit elliptic curve group (ECP)
- Encryption: Advanced Encryption Standard (AES)-256
- Hash: Secure Hash Algorithm (SHA)-384

Diffie-Hellman Group 15 is also acceptable based on the minimum requirements of CNSSP 15, but Group 15 is not recommended due to interoperability issues that have been observed.

When establishing a VPN proposal, policy, or transform-set, ensure it follows CNSSP 15 recommendations [4]. The CNSSP 15 requirements are explained in the draft Internet Engineering Task Force (IETF) document on "Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec)" [5].

To ensure they are not inadvertently used, disable the default polices and proposals for Internet Security Association and Key Management Protocol (ISAKMP) and IKEv2 with the following configuration commands:

```
no crypto isakmp default policy
no crypto ikev2 policy default
no crypto ikev2 proposal default
no crypto ipsec transform-set default
```

Note: If the default policies are disabled, only the explicitly configured policies will be used.

Establish an IKEv2 proposal, policy, and profile with the following example configuration commands:

```
crypto ikev2 proposal <IKEV2_PROPOSAL_NAME>
 encryption aes-gcm-256
 group [16|20]

crypto ikev2 policy <IKEV2_POLICY_NAME>
 proposal <IKEV2_PROPOSAL_NAME>

crypto ikev2 profile <IKEV2_PROFILE_NAME>
 match identity remote ...
 authentication remote ...
 authentication local ...
```

The configuration of the profile will depend on the network it is configured for, and must have local and remote authentication methods and a `match` statement. A separate keyring can also be established and applied to the profile for multiple pre-shared keys.

Establish an IPsec transform-set with the following example configuration commands:

```
crypto ipsec transform-set <IPSEC_TRANSFORM_NAME> esp-gcm 256
 mode tunnel
```

Establish an IPsec profile, which utilizes the IKEv2 profile and IPsec transform-set defined above, with the following example configuration commands:

```
crypto ipsec profile <IPSEC_PROFILE_NAME>
 set transform-set <IPSEC_TRANSFORM_NAME>
 set pfs group16
 set ikev2-profile <IKEV2_PROFILE_NAME>
```

The IPsec profile should be applied to the tunnel interface with the following configuration commands:

```
interface <TUNNEL_INTERFACE_NAME>
 tunnel protection ipsec profile <IPSEC_PROFILE_NAME>
 no shutdown
```

For more information, refer to "Configuring IPsec Virtual Private Networks," "Mitigating Recent VPN Vulnerabilities," and "Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations" [6], [7], [8].

Return to Contents

3. Security maintenance

Outdated hardware and software may contain publicly known vulnerabilities and provide an easy mechanism for adversaries to exploit the network. These vulnerabilities are mitigated by regularly upgrading the hardware and software to newer versions that are supported by the vendor. Additionally, the integrity of downloaded software should be verified before and during use. Security maintenance should be performed on a regular basis to ensure devices continue to operate securely.

Upgrade hardware and software to ensure efficiency and security.

3.1 Verify software and configuration integrity

An adversary can introduce malicious software into network devices by modifying operating system files, the executable code running in memory, or the firmware or bootloader that loads the operating system of a network device. Software that has been maliciously modified on a network device can be used by an adversary to violate data integrity, exfiltrate sensitive information, and cause a denial of service (DoS).

NSA recommends verifying the integrity of operating system files installed and running on devices by comparing the cryptographic hash of the file with the known good hash published by the vendor. When upgrading operating system files, perform the same integrity verification on the files prior to and after installation to ensure no modifications were made. A basic online hash can be computed on an operating system image file with the following exec command:

```
verify /sha512 <PATH:filename>
```

Older devices may only support a Message Digest 5 (MD5) hash, which can be computed with the following exec command:

```
verify /md5 <PATH:filename>
```

The computed hash can be compared with the information published for the file on the Support pages of https://www.cisco.com/ [12]. More information on network device verification is available in the "Network Device Integrity (NDI) Methodology," "Network Device Integrity (NDI) on Cisco IOS Devices," and "Validate Integrity of Hardware and Software" documents [30], [31], [32].

Rather than performing these more complex software modifications, an adversary may choose to simply change the configuration. Configuration changes can be a sign that a device has been compromised.

NSA also recommends implementing a configuration change control process that securely creates device configuration backups to detect unauthorized modifications. When a configuration change is needed, document the change and include the authorization, purpose, and mission justification. Periodically verify that modifications have not been applied by comparing current device configurations with the most recent backups. If suspicious changes are observed, verify the change was authorized.

3.2 Maintain proper file system and boot management

Many network devices have at least two different configurations, one or more saved in persistent storage and an active copy running in memory. Permanent changes to the configuration should be saved or committed to prevent configuration inconsistencies if the device is rebooted or loses power. Configuration changes can be saved on a device with the following exec command:

```
copy running-config startup-config
```

If changes are meant to be temporary, NSA recommends inserting comments before the updated configuration lines to include why it was made and when it can be removed, and removing the comments and temporary changes at the appropriate time. If the device does not support comments, insert comments in a backup copy of the configuration to compare with the version on the device.

Use an encrypted protocol when copying configurations remotely, such as Secure File Transfer Protocol (SFTP) or Secure Copy Protocol (SCP). The copy mechanism used to backup or archive configurations, and the backup repository, must be protected from unauthorized access.

NSA also recommends checking for unused or unnecessary files on each device and removing them with the following exec commands:

```
dir /recursive all-filesystems
delete <PATH:filename>
```

Older operating system files or outdated backup configuration files stored on the device are most likely unnecessary, and should be removed. Storing multiple versions of software provides an adversary the opportunity to reload outdated software and reintroduce vulnerabilities patched in newer versions of the operating system.

3.3 Maintain up-to-date software and operating systems

Maintaining up-to-date operating systems and stable software protects against critical vulnerabilities and security issues that have been identified and fixed in newer releases. Devices running outdated operating systems or vulnerable software are susceptible to a variety of published vulnerabilities, and exploiting these devices is a common technique used by adversaries to compromise a network.

NSA recommends upgrading operating systems and software on all devices to the latest stable version available from the vendor. Upgrading the operating system may require additional hardware or memory upgrades, and obtaining a new software version may require a maintenance or support contract with the vendor. Some network infrastructure devices may not support an auto-update feature, so it may be necessary to implement a requisition and installation process to obtain the latest software from the vendor.

Please see the support page for the corresponding vendor in *Table I: Vendor support pages* to determine the latest operating system for a particular device.

Table I: Vendor support pages

Vendor	URL
Arista Networks	https://www.arista.com/en/support/ [9]
Aruba Networks	https://www.arubanetworks.com/support-services/ [10]

Vendor	URL
Broadcom	https://www.broadcom.com/support [11]
Cisco Systems	https://www.cisco.com/c/en/us/support/index.html [12]
Dell	https://www.dell.com/support/home/en-us/ [13]
Extreme Networks	https://www.extremenetworks.com/support/ [14]
F5	https://www.f5.com/services/support [15]
Fortinet	https://www.fortinet.com/support [16]
Hewlett Packard Enterprise (HPE)	https://www.hpe.com/us/en/services.html [17]
International Business Machines (IBM)	https://www.ibm.com/mysupport/ [18]
Juniper Networks	https://support.juniper.net/support/ [19]
Linksys	https://www.linksys.com/us/support/ [20]
NETGEAR	https://www.netgear.com/support/ [21]
Palo Alto Networks	https://support.paloaltonetworks.com/support/ [22]
Riverbed Technology	https://support.riverbed.com/ [23]
Ruckus Networks	https://support.ruckuswireless.com/ [24]
SonicWall	https://www.sonicwall.com/support/ [25]
TRENDnet	https://www.trendnet.com/support/ [26]
Tripp Lite	https://www.tripplite.com/support/ [27]
Ubiquiti	https://help.ui.com/hc/en-us/ [28]
WatchGuard	https://www.watchguard.com/wgrd-support/overview [29]

3.4 Stay current with vendor-supported hardware

Vendors eventually stop supporting specific hardware platforms and, if a failure occurs, these end-of-life devices cannot be serviced. In addition to device instability and memory requirement concerns, there is an increased risk of an adversary exploiting the device due to a lack of software updates to fix known vulnerabilities. Newer, vendor-supported hardware platforms have improved security features, including protection from known vulnerabilities.

Once a vendor publishes an end-of-life notice or announces that a device will no longer be supported, NSA recommends constructing a plan to upgrade or replace affected devices with newer equipment, according to vendor recommendations. Outdated or unsupported devices should be immediately upgraded or replaced to ensure the availability of network services and security support.

Please see the support page for the corresponding vendor in *Table I: Vendor support pages* to determine if a particular device is supported by the vendor.

Return to Contents

4. Authentication, authorization, and accounting (AAA)

Centralized AAA servers provide a consolidated mechanism to manage administrative access to devices, and the accounts created are more challenging for an adversary to compromise since credentials are not stored directly on devices. Properly configuring these servers provides an authoritative source for managing and monitoring access, improves consistency of access control, reduces configuration maintenance, and reduces administrative costs. All devices should first be configured to use modern AAA services with the following configuration example command for Cisco IOS devices:

Control access and reduce maintenance through use of AAA.

```
aaa new-model
```

Applying the above configuration ensures a device will not use legacy authentication and authorization methods.

4.1 Implement centralized servers

All devices should be configured to use centralized AAA servers. NSA recommends implementing at least two AAA servers to ensure availability, and assist with detecting and preventing adversary activities. If one server becomes unavailable due to scheduled maintenance or for other reasons, the remaining servers will continue providing the centralized AAA services. The servers should be:

- Configured to authenticate devices with a unique and complex pre-shared key to ensure only authorized devices can use the AAA services (see 5.5 Create strong passwords).
- Configured to use the same protocol (e.g., TACACS+, RADIUS, or LDAP) for consistency, and use encrypted transport when supported (e.g., RadSec, Diameter, LDAPS, or IPsec encapsulated).
- Synchronized with each other to ensure consistency of user credentials and access controls.

A server group with multiple AAA servers can be configured with the following configuration commands:

```
aaa group server {tacacs+ | radius | ldap} <GROUP_NAME>
 server-private <IP_ADDRESS_1> key <KEY_1>
 server-private <IP_ADDRESS_2> key <KEY_2>
```

Some older devices may utilize the keywords `tacacs-server` and `radius-server` in the configuration, which prevents assigning a unique key to each server.

NSA recommends replacing these lines with the above configuration format, and assigning a unique pre-shared key to each server. If an adversary obtains the pre-shared key to one server, the key needs to be revoked, but other servers with different keys can continue to be used by the devices.

4.2 Configure authentication

Authentication verifies the identity of a person or entity. All devices should be configured to use centralized servers for AAA services first, and local administrator accounts as a backup method only if all the centralized servers are unavailable. The same applies to privileged level authentication; devices should only use the local privileged-level password if all centralized servers are unavailable. This order of precedence will prevent an adversary, who obtains local administrator account credentials, from logging into the devices since access will usually be controlled by the AAA servers.

NSA recommends configuring centralized authentication for `login` and `enable` (privileged) access as the primary method, as shown in the following configuration commands:

```
aaa authentication login default group <GROUP_NAME> local
aaa authentication enable default group <GROUP_NAME> enable
```

Using the `default` keyword ensures the configuration is applied globally in all instances when an explicit authentication list is not specified. If a custom named list is used instead, it would be necessary to explicitly apply this list to all instances where AAA is used and potentially leave some management services incorrectly configured and open to compromise. The `default` list is always applied when a custom named list is not explicitly applied.

The *<GROUP_NAME>* should be the custom name of the AAA server group (defined previously) that includes the IP addresses of the centralized AAA servers and their associated keys.

The `line` keyword should not be used as these passwords are not securely stored in the configuration and do not provide accountability.

The `none` keyword should never be used since it disables authentication.

4.3 Configure authorization

Authorization validates that a person or entity has permission to access a specific resource or perform a specific action. The organization, situation, and the device's purpose will dictate authorized administrator commands. At the least, authorization should be applied to starting an exec session (shell) and execution of other shell commands, including configuration commands. Authorization should also be explicitly applied to the console, as it may not be automatically applied by default.

NSA recommends adequately restricting what legitimate administrators are authorized to execute to prevent an adversary from performing unauthorized actions with a compromised account. Most administrators use privilege level 1 for user level access and privilege level 15 for privileged level access.

Authorization should be applied to both of these levels and any other privilege levels used by administrators with the following configuration commands:

```
aaa authorization console
aaa authorization exec default group <GROUP_NAME> local
aaa authorization commands 1 group <GROUP_NAME> local
aaa authorization commands 15 group <GROUP_NAME> local
aaa authorization config-commands
```

The `default` list should be used to ensure the configuration is applied everywhere.

The *<GROUP_NAME>* should be the custom name of the AAA server group (defined previously) that includes the IP addresses of the centralized AAA servers and their associated keys.

If desired, the `if-authenticated` keyword can be applied after the `local` keyword. If an administrator is successfully logged in and all the centralized AAA servers become unavailable, the administrator will no longer be authorized to execute commands. The `if-authenticated` keyword ensures an authenticated user will continue to be authorized to execute commands. However, be cautious with this keyword as it could

potentially give an administrator access beyond what is configured on the centralized AAA servers.

The `none` keyword should never be used since it disables authorization.

4.4 Configure accounting

Accounting keeps records of all relevant resources accessed or actions performed, holding administrators accountable. Waiting until an event is stopped to generate an accounting record is insufficient, as a particular action could take an unreasonable amount of time to complete before the record is generated. Accounting records can be collected for several other event types, but it depends on the organization and purpose of devices.

NSA recommends that system configuration changes be centrally recorded, and a process implemented to periodically review these records to detect potential malicious activities. At a minimum, accounting records should be collected when an exec session (shell) is started and stopped, and when shell commands are started and stopped. Similar to authorization, accounting of `commands` must be applied to all administrator privilege levels with the following configuration commands:

```
aaa accounting exec default start-stop group <GROUP_NAME>
aaa accounting commands 1 default start-stop group <GROUP_NAME>
aaa accounting commands 15 default start-stop group <GROUP_NAME>
```

The `default` list should be used to ensure the configuration is applied everywhere.

The *<GROUP_NAME>* should be the custom name of the AAA server group (defined previously) that includes the IP addresses of the centralized AAA servers and their associated keys.

4.5 Apply principle of least privilege

Least privilege is a security concept that authorizes access to a person or entity at the lowest privilege level necessary to perform authorized tasks. Many common tasks do not require privileged level access, such as viewing status of network interfaces or reviewing routing tables. To implement least privilege, administrators should initially log in with the lowest privilege level necessary. This provides an additional layer of security

that an adversary must circumvent to fully compromise a device. It also prevents administrators from inadvertently making configuration changes to a device.

NSA recommends that all accounts be configured with privilege level 1 or 0, and require administrators to enter additional credentials to elevate to a higher privilege level to perform required tasks. Privilege levels should be periodically reviewed, and unnecessary accesses removed to prevent inadvertent use of privileged level commands at lower privilege levels.

The privilege level of individual local accounts can be changed with the `privilege` keyword. Assign local accounts to privilege level 1 with the following configuration command:

```
username <USER_NAME> privilege 1
```

Note: This does not change the account password.

All administrator accounts logging in at privilege level 1 will be required to execute the `enable` command and provide additional credentials to elevate to a higher privilege level. In addition to reviewing all local administrator accounts and ensuring they are assigned the least privilege level, it is also necessary to review all accounts configured on the centralized AAA servers.

Similarly, the same concept should be applied to the console (CON), auxiliary (AUX), and virtual teletype (VTY) lines. When AAA authorization is properly configured, it should not be dependent on the configuration of the lines. However, it is a best practice to ensure the lines are configured to the least privilege level with the following configuration commands:

```
line con 0
 privilege level 1

line aux 0
 privilege level 1

line vty 0 4
 privilege level 1

line vty 5 15
 privilege level 1
```

Depending on the device, it may be necessary to apply a similar configuration to other lines as well. If VTY lines 5 through 15 do not exist on a particular device, it is not necessary to execute those commands.

4.6 Limit authentication attempts

Limiting the number of authentication attempts and introducing a login delay prevents an adversary from performing brute force password cracking against a device in an attempt to obtain access.

NSA recommends restricting failed remote administration attempts to a maximum of three or less with the following configuration example command for Cisco IOS devices:

```
aaa authentication attempts login 3
```

Similarly, the same concept of three or less failed attempts should be applied to Secure Shell (SSH) sessions with the following configuration command:

```
ip ssh authentication-retries 3
```

NSA also recommends introducing a delay of at least one second between login attempts to significantly slow down brute force attempts with the following configuration command:

```
login delay 1
```

Return to Contents

5. Local administrator accounts and passwords

Local accounts are vital to the management of network devices. If centralized authentication fails, the local accounts provide administrators with access to the network devices to troubleshoot and diagnose network issues. Local accounts should be unique, authenticated with a unique and complex password, and provide accountability for individual administrators. If a password policy does not exist for the organization, establish and enforce a new policy. Periodically review and revise the policy, when necessary.

Create unique local accounts with complex passwords.

This section focuses primarily on local accounts and passwords. Traditional network devices use legacy methods for managing local accounts, and they may not support the recommended mechanisms for composing, changing, and verifying passwords. The simplistic nature of these local accounts requires different recommendations to be applied. This is in contrast to the centralized AAA servers where multi-factor authentication, password complexity, previous password comparison, and other concepts can be properly implemented.

5.1 Use unique usernames and account settings

Most devices have default administrative credentials which are advertised to the public, and they often grant full administrative access to a device. Maintaining these settings offers the adversary an easy entry into the network to connect and potentially gain privileged level access to anonymously monitor or reconfigure the device.

NSA recommends removing all default configurations and reconfiguring each device with a unique and secure account for each administrator. Do not introduce any new devices into the network without first changing the default administrative settings and accounts.

Note: The default user account on some devices cannot be removed.

Accounts can be used by individual administrators or shared among a group. However, if multiple administrators use a group account to access the device, accountability cannot be enforced as configuration changes will not be associated to a specific individual. For this reason, adversaries target group accounts to gain unauthorized access to devices.

NSA further recommends disabling all shared or group administrator accounts, and using a unique account for each administrator to provide access for configuration changes and to ensure accountability on each device. If group accounts are necessary, NSA recommends monitoring these accounts to detect any suspicious activity. It may not be feasible to create a backup local account for each administrator, but a single group account known to every administrator does not provide individual accountability.

NSA also recommends that local accounts only be used in emergency situations when the centralized AAA servers are unavailable. Unique local emergency account passwords should be maintained by a trusted individual who does not have direct

access to the devices. During an event, administrators can request the local account and password and, once the emergency situation has ended, the trusted individual can then change the password. This will prevent password reuse and ensure accountability. All other authentication requests should occur via the centralized AAA servers.

5.2 Change default passwords

Most devices are assigned a default password, or sometimes no password, to allow an administrator easy access prior to initial configuration. Many of these passwords are public knowledge and typically do not need to be changed for the device to work properly. They are prime targets for malicious automated scanners (botnets) to exploit, as the default credentials provide privileged level access to the device.

NSA recommends removing all default passwords and assigning a unique, complex, and secure password to all levels of access, including both user and privileged levels. Additionally, when introducing new devices into the network, change the default user and privileged level passwords before attaching the device to the network.

5.3 Remove unnecessary accounts

Some devices are configured with unnecessary accounts by default. Since they may be rarely used or not used at all, these accounts are often overlooked. If possible, rename or remove default accounts that are not associated with a particular administrator.

NSA recommends that the number of accounts authorized to log onto devices should be limited to what is necessary; all others should be removed. When an administrator leaves an organization or changes roles, the associated accounts should be disabled or removed. On Cisco IOS devices, remove a local account with the following configuration command:

```
no username <NAME>
```

5.4 Store passwords with secure algorithms

Passwords are generally stored in the configuration of a device or in a local database, as clear text, encrypted, or a one-way hash. Clear text should never be used, and some encryption or hash functions are considered weak and could easily be broken using publicly available tools. An adversary could accumulate passwords or hashes from the configuration or local database by using a network analyzer or by compromising a central management system that stores configuration files. The clear text and weak

algorithm passwords could be easily cracked and used to obtain user or privileged level access to a device. Cisco IOS supports the following one-way hash and encrypted types:

- **Type 0** passwords should not be used because they are stored in clear text
- **Type 4** password hashes should not be used because they are easy to crack
- **Type 5** (MD5) password hashes should be avoided except on older operating systems that do not support Types 6, 8, or 9
- **Type 6** passwords are AES-encrypted and should only be used for passwords that need to be encrypted instead of hashed (such as for VPN keys), or on systems that do not support Type 8 (which typically implies that Type 9 is also unavailable)
- **Type 7** passwords should not be used because they are easily reversible, even though they are encrypted
- **Type 8** (SHA-256 PBKDF2) password hashes are recommended
- **Type 9** (Scrypt) password hashes are not approved by the National Institute of Standards and Technology (NIST)

For more information on the above password types, see "Cisco Password Types: Best Practices" [33].

NSA recommends that all passwords on a device be stored using the most secure algorithm available, and never stored as clear text. One-way hash algorithms are irreversible and generally should be used for storing passwords. However, if one-way hash algorithms are unavailable, the passwords should be encrypted with a strong unique key.

When creating a user account or assigning a password, some devices require the algorithm to be specified. Special attention should be given to privileged level accounts, but this guide also applies to user accounts, management ports, authenticated routing protocols, VPN keys, and any place where a password may be specified in the device's configuration.

Prevent clear text passwords with the following configuration command:

```
service password-encryption
```

Store a Type 8 password hash for a local account with the following configuration command:

```
username <NAME> algorithm-type sha256 secret <PASSWORD>
```

Note: The `algorithm-type` keyword is not stored in the saved configuration in `nvram:/startup-config`; instead the `secret` keyword is replaced with `secret 8` prior to the hashed password.

If reversible encrypted passwords are needed (such as for VPN keys), use Type 6 AES instead of Type 7 passwords with the following configuration commands:

```
password encryption aes
key config-key password-encrypt <KEY>
```

The *<KEY>* should be a unique and complex password that is used to generate the key to encrypt Type 6 passwords. It should not be a default, weak, or easily guessable password, and should not be reused elsewhere in the configuration. An adversary that guesses this key could use it to decrypt all Type 6 passwords stored in the configuration. Once this key is set, it generally does not need to be retained.

Note: The `key config-key password-encrypt` configuration command is not stored in the saved configuration in `nvram:/startup-config`.

Since it does not need to be retained, NSA recommends using a unique key for every device which will prevent an adversary from using the same key to decrypt the Type 6 passwords on all of the devices.

Note: If the key is ever changed, the Type 6 encrypted passwords will need to be manually set again.

5.5 Create strong passwords

A device configured with a weak password increases an adversary's ability to compromise that device. An adversary may be able to easily guess a weak password or crack it using publicly available password cracking tools (e.g., dictionary or brute force attempts). Once privileged level access is obtained, an adversary can make configuration changes that potentially compromise other devices on the network.

NSA recommends assigning a unique and complex password to all levels of access, including both user and privileged level accesses. Unique and complex passwords should also be used for routing authentication, time synchronization, VPN tunnels, Simple Network Management Protocol (SNMP) community strings, and anywhere else passwords are stored in the configuration. Passwords should meet the following complexity requirements:

- Use all the different character classes (uppercase, lowercase, numbers, and special characters)
- Be at least 15 characters long
- Not be based on unmodified words or acronyms
- Not be a keyboard walk
- Not be the same as a username
- Not be related to the network, organization, location, local sports team, or other function identifiers
- Not be identical or similar to the last password or passwords assigned elsewhere
- Not be a default, blank, or publicly known password

An organization's password policy may not require passwords managed through the centralized AAA servers to adhere to all of these recommendations, especially when coupled with multi-factor authentication and other principals. The above guidance should at least be applied to local accounts and other passwords that are stored in the configuration of a network device, where centralized security controls cannot be applied.

NSA highly discourages using SNMP version 1 or 2c. For more information, refer to 7.1 Disable clear text administration services and 7.8 Remove SNMP read-write community strings.

An adversary with knowledge of the network, location, programs, etc. could easily guess (or know) these terms, thus aiding them in cracking the passwords.

NSA also recommends checking for weak passwords on a regular basis to enforce the organization's password policy. Password complexity should be checked before setting a new password. Network administrators should periodically review network device configurations to identify the use of weak password algorithms.

5.6 Utilize unique passwords

Assigning the same password to multiple accounts or multiple levels of access could impact accountability and authorization. If an administrator accesses the device via an unencrypted protocol, an adversary could use a network analyzer to collect the password from network traffic. If an adversary gains user level access, they could potentially reuse the same password to also gain privileged level access.

Assigning the same password to multiple devices allows an adversary to compromise numerous devices at the same time, without any extra effort. If the same password was assigned to a majority of the devices, an adversary would only need to compromise a single password to obtain privileged level access to all of those devices.

NSA recommends assigning a unique, complex, and secure password for each account and privileged level on each device.

NSA also recommends checking for password reuse across multiple accounts and levels of access, and across multiple devices. Identical hashes can be an indication of password reuse.

5.7 Change passwords as needed

Periodically changing passwords has historically led to the use of weaker passwords, and enforcing this policy may not be necessary if users follow the guidance in 5.5 Create strong passwords. The initial creation of strong passwords is a more effective method of reducing successful password compromises.

NSA recommends changing a password immediately if the password or password hash has been compromised, and storing it securely as described in 5.4 Store passwords with secure algorithms. Given enough time and resources, every password can be guessed or brute force cracked, which is an attempt at all possible character combinations. Compromised passwords that have not been changed give an adversary even more time to use these techniques. Additionally, if an adversary eventually cracks an old password, they may continue attempting variations and guess the current password if it was based on a previous password.

Unfortunately, it can be difficult to discern when a password has been compromised, especially local passwords stored in the configuration. Traditional network devices are significantly more simplistic in how they store and transmit the configuration, which

includes passwords and password hashes. Furthermore, emailing network device configurations or storing them in unprotected file shares could constitute a compromise, because the passwords and password hashes stored in the configurations are left unprotected. Additionally, passwords stored with a weak algorithm should be considered compromised, since they are significantly easier to crack.

If the confidentiality of passwords cannot be maintained or the organization desires to regularly attempt to evict actors who may have compromised passwords without being detected, NSA recommends establishing an aging policy that incorporates changing passwords on a regular basis. Changing local passwords can be significantly more cumbersome than centralized passwords, so it is necessary to choose a time frame that is reasonably practical for network administrators to follow, while reducing the amount of time an adversary can utilize a potentially compromised password. If the device does not support long passwords, it is recommended that passwords be changed more frequently to prevent an adversary from cracking a password that is still in use.

Note: If a password is stored using a convoluted Type 9 secret where the `secret 9` password hash begins with `$14$`, it indicates that the password was not recently changed. The password hash was converted from Type 5 during a previous operating system upgrade. The convoluted Type 9 secret should be removed by changing the password to a Type 8 secret with the `algorithm-type sha256` keywords, as previously described in 5.4 Store passwords with secure algorithms.

Return to Contents

6. Remote logging and monitoring

Logging is an important mechanism for recording device activities and tracking network security events. It provides administrators with the ability to review the logs for suspicious activities and to investigate incidents. An incomplete logging configuration on a device can lead to missing or inaccurate information and difficulty correlating events that occurred on a device or the network. Proper logging includes sending logs to multiple remote log servers, synchronizing the clock to multiple authenticated time sources, and implementing log management policies and procedures. A security information and event management (SIEM)

Enable and configure logging to identify malicious activity.

system can be used to aggregate and analyze logs received by the remote log servers. Logs should be retained as recommended by the Office of Management and Budget (OMB) Memorandum M-21-31 [34].

6.1 Enable logging

Log messages will only be generated on network devices when logging is enabled. Devices should be configured to send log messages to a local log buffer and centralized log servers simultaneously.

NSA recommends enabling syslog logging, setting the local log buffer to 16 megabytes or greater, and establishing a procedure to verify the logs are received and reviewed on a regular basis. Most devices should be able to support the larger buffer size, but it can be decreased for a particular device if there is insufficient memory.

Ensure that syslog logging is enabled with the following configuration command:

```
logging on
```

Increase the maximum local log buffer with the following configuration command:

```
logging buffered 16777216 informational
```

Note: This will also change the logging level to informational, as both values must be set simultaneously.

6.2 Establish centralized remote log servers

Log messages sent to remote log servers are less vulnerable to compromise or erasure, ensuring that the messages will not be impacted in the event a device is compromised, rebooted, or the local log buffer becomes full. Multiple log servers are critical when defending against DoS effects and reducing a single point-of-failure.

NSA recommends establishing at least two remote, centralized log servers to ensure monitoring, redundancy, and availability of device log messages. If supported, ensure the log messages are encrypted in transit to prevent unauthorized disclosure of sensitive information. Outbound syslog messages can only be encrypted on a Cisco IOS device by creating an IPsec tunnel between the device and the remote syslog servers, as described in 2.6 Limit and encrypt virtual private networks (VPNs). Configure at least two remote log servers with the following configuration commands:

```
logging host <IP_ADDRESS_1>
logging host <IP_ADDRESS_2>
```

6.3 Capture necessary log information

Devices configured with sufficient information in the logs provide administrators with the information they need to analyze events related to an incident, including correlating multiple events or events occurring on other devices.

NSA recommends setting the trap and buffer logging levels on each device to at least syslog level “informational” (code 6) to collect all necessary information. Devices can be configured for “debugging” (code 7), but the increased number of generated messages may slow down the log review process. Set both the trap and buffer logging levels to informational with the following configuration commands:

```
logging trap informational
logging buffered 16777216 informational
```

Note: This will also set the maximum size of the local log buffer, as both values must be set simultaneously.

Logging can also be enabled on the console and VTY lines with the `console` and `monitor` keywords, respectively. These methods will immediately alert administrators that are logged in, but the messages are not retained. It is not necessary to enable logging for these methods unless it is desired by the administrators. These logging mechanisms can be disabled with the following configuration commands:

```
no logging console
no logging monitor
```

NSA also recommends using Coordinated Universal Time (UTC) for the time zone, especially if the network spans multiple time zones. All log messages should contain a properly configured timestamp with the full date including the year, the time including seconds and milliseconds, and the time zone. Ensure the time zone is properly set and enable all the features listed above with the following configuration commands:

```
clock timezone UTC 0 0
service timestamps log datetime msec localtime show-timezone year
service timestamps debug datetime msec localtime show-timezone year
```

Finally, NSA also recommends enabling log messages to indicate when a user was successful or unsuccessful at logging into the system. Even though these events are recorded on the centralized AAA servers when accounting is properly configured, this information is not logged in the local buffer. Ensure these events are logged with the following configuration commands:

```
login on-failure log
login on-success log
```

6.4 Synchronize clocks

The Network Time Protocol (NTP) is used to synchronize device clocks worldwide and to ensure that the timestamps included with log messages are reasonably accurate. To provide this reliability, each device should synchronize with at least two trusted time sources. This accuracy is critical to ensure log message timestamps can be easily correlated across geographically dispersed time zones, and used to collectively trace a network incident from one device to another.

NSA recommends that each device and the remote log servers use at least two trustworthy and reliable time servers to ensure accuracy and availability of information. Internal time servers should be established as the primary source for all devices, which should subsequently synchronize with authoritative external sources. This design decreases the number of external requests and ensures consistency of timestamps in the event an external time server is unreachable. When deploying time servers on the network, administrators should confirm that devices can access the time servers, and that the clocks are synchronized after the configuration has been applied.

NSA also recommends enabling NTP authentication on all devices to prevent clock tampering, and configuring strong, unique NTP authentication keys between the devices and their specified time source.

Establish the trusted NTP keys and enable NTP authentication with the following configuration commands:

```
ntp authentication-key <#1> md5 <KEY>
ntp trusted-key <#1>
ntp authentication-key <#2> md5 <KEY>
ntp trusted-key <#2>
ntp authenticate
```

Any number of trusted keys can be established. Note that NTP authentication keys will be stored in the configuration as Type 7 passwords. Type 6 AES-encrypted passwords are not supported for NTP authentication.

Synchronize the device with at least two different NTP servers with the following configuration commands:

```
ntp server <IP_ADDRESS_1> key <#1>
ntp server <IP_ADDRESS_2> key <#2>
```

Note: The number at the end of each command is the trusted NTP key used to authenticate that particular server.

After waiting for the clock to synchronize, verify synchronization and status of the NTP servers with the following exec commands:

```
show ntp status
show ntp associations
```

Note: It is necessary to verify clock synchronization after every NTP configuration change, and it may take several hours for proper synchronization.

Return to Contents

7. Remote administration and network services

Protect your network management tools from adversaries.

Network devices can be managed remotely by administrators through various services. Some common network services include SSH, Hypertext Transfer Protocol (HTTP), SNMP, and File Transfer Protocol (FTP). These services are useful for administrators, but they are also targeted by adversaries to exploit and gain privileged level access to a device. All of them must be properly configured to reduce the probability of a compromise.

7.1 Disable clear text administration services

Clear text protocols pass traffic across the network “in the clear” (i.e., unencrypted) and were designed prior to widespread use of encryption. Therefore, using these protocols to remotely administer critical devices may lead to an information disclosure that could

adversely affect device and network security. An adversary could compromise a device or service by collecting usernames, passwords, configuration information, and other sensitive data through common information retrieval techniques (e.g., network analyzer or packet capture utility).

NSA recommends using encrypted services to protect network communications and disabling all clear text administration services (e.g., Telnet, HTTP, FTP, SNMP 1/2c). This ensures that sensitive information cannot be easily obtained by an adversary capturing network traffic. For detailed information on how to enable encrypted services, refer to 7.11 Configure remote network administration services.

If a device does not support encrypted protocols, connect a management system directly to the console or management port, or establish a dedicated out-of-band management network to reduce the ability of an adversary capturing the clear text protocols. Disable the Telnet service with the following configuration commands:

```
line vty 0 4
 transport input none

line vty 5 15
 transport input none
```

Depending on the device, it may be necessary to apply a similar configuration to other lines as well. If VTY lines 5 through 15 do not exist on a particular device, it is not necessary to execute those commands.

Note: These commands may also disable other services that are enabled on the lines by default, including SSH. For detailed information on how to enable SSH, refer to 7.11.1 Configuring SSH for remote administration.

Disable the HTTP service with the following configuration command:

```
no ip http server
```

For detailed information on how to enable the secure HTTP service, refer to 7.11.2 Configuring HTTP for remote administration.

Disable versions 1 and 2c of the SNMP and SNMP trap services by removing any configured community strings with the following configuration commands:

```
no snmp-server community <COMMUNITY_STRING>
no snmp-server host <HOSTNAME_OR_IP_ADDRESS> <COMMUNITY_STRING>
```

For detailed information on how to enable SNMP version 3, refer to 7.11.3 Configuring SNMP for remote administration.

Disable the Trivial File Transfer Protocol (TFTP) by removing any lines with the following configuration command:

```
no tftp-server <FILENAME>
```

The FTP service is generally not enabled as a listening service, but the protocol can be used as a client. Remove FTP credentials with the following configuration commands:

```
no ip ftp username
no ip ftp password
```

7.2 Ensure adequate encryption strength

Some encrypted services require that a public and private key pair be generated so clients can connect and authenticate to the server. Additionally, the client and server of an encrypted connection may collectively establish a private session key for each unique connection. Encrypted connections that use weak algorithms or a small number of bits make it easier for an adversary to crack the private session key and decrypt all of the data transferred during a unique connection.

For guidance on which algorithms and ciphers are NSA-approved for National Security Systems (NSS), refer to CNSSP 15 [4]. The CNSSP 15 requirements are explained in the draft IETF documents on Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec), Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3, and Commercial National Security Algorithm (CNSA) Suite Cryptography for Secure Shell (SSH) [5], [35], [36].

For related requirements and guidance for non-NSS U.S. Government systems, refer to NIST SP 800-52 Revision 2 Appendix F [37].

These documents contain the latest recommended encryption parameters.

NSA recommends that 3072 bits or higher be used for asymmetric (public and private) key generation, 384 bits for elliptic curve cryptography (ECC) keys, and 256 bits for symmetric encryption keys. Some systems may not support 3072 bits, so it may be necessary to use 4096 bits instead. For any device that has a smaller key size, regenerate a new key pair and configure encrypted protocols to only use approved algorithms. A larger key size may increase the time to connect to the service (due to extra computations), but is negligible on most devices. For more information on configuring encrypted services, refer to 7.11 Configure remote network administration services.

7.3 Utilize secure protocols

Several common administration services implement protocols that contain flaws in the implementation and exchange of information, which can be exploited by an adversary. Some protocols, such as SSH, can be configured to be backward compatible and accept older insecure protocols, along with the newer ones. Older protocols are subject to man-in-the-middle techniques that can force clients and servers to negotiate weaker algorithms, possibly without user awareness.

NSA recommends ensuring administration services are using the latest version of protocols, with the proper security settings adequately enabled. SSH version 2 is the preferred method for remotely accessing devices. Encrypted HTTP servers should be configured to only accept Transport Layer Security (TLS) version 1.2 or higher. For more information on limiting services to specific versions of the protocol, refer to 7.11 Configure remote network administration services.

7.4 Limit access to services

If a large number of devices are permitted to connect to management services, they are more vulnerable to exploitation. NSA recommends configuring ACLs to allow only administrative systems to connect to devices for remote management. Devices that do not have the capability to support ACLs should be placed on a separate network management segment (e.g. VLAN).

Once created, an ACL should be applied to that VLAN or at the ingress router to restrict access to this network segment. It may be necessary to implement a separate firewall in front of critical network segments to restrict what systems can connect to that VLAN. Consider using Dynamic Host Configuration Protocol (DHCP) with reserved IP

addresses, or assigning administrative systems with static IP addresses, to make it easier to define the ACL and limit administrative access to the management services.

Most management services only accept standard ACLs. More than one device or network can be listed on additional lines with the `permit` keyword. Even though every ACL has an implied `deny` statement at the end, it is a best practice to explicitly include it so denied attempts are logged. Create a standard ACL to only permit IP addresses used by administrators with the following configuration commands:

```
access-list <ACL#> permit <NETWORK> <WILDCARD_MASK> log
access-list <ACL#> deny any log
```

For more information on how to apply ACLs to specific administrative services, refer to 7.11 Configure remote network administration services.

NSA also recommends removing unused ACLs from the configuration to reduce confusion around whether or not they are properly applied. After verifying that a standard ACL is not applied, remove it with the following configuration command:

```
no access-list <ACL#>
```

7.5 Set an acceptable timeout period

Setting a timeout period for idle connections allows sessions to close after a prescribed time of inactivity. When timeout periods are not set or set too long, it is possible for idle connections to continue indefinitely or even cause a DoS if limited simultaneous connections have been set on the device. The DoS will persist until the idle timeout period has been reached, which could be indefinite if the idle timeout has been disabled. A longer timeout period provides an adversary with more time to hijack a session while it is idle.

NSA recommends setting the session timeout for administrative connections to five minutes or less on all remote devices (e.g., exec-timeout on VTY lines, SSH, console and auxiliary ports). Do not set the timeout period to zero, as most devices will disable the timeout function with this setting. For more information on limiting the session timeout on specific administrative services, refer to 7.11 Configure remote network administration services.

7.6 Enable Transmission Control Protocol (TCP) keep-alive

TCP keep-alive messages sent and received from a device allow it to assess the connection status when no activity has occurred in a given timeframe. These messages can be used to detect an inadvertent loss in connection and mitigate against potential network compromises. On some devices, the lack of a TCP keep-alive service causes established TCP connections to remain open after an inadvertent connection loss on one end, leaving the session vulnerable to hijacking. Additionally, authentication may not even be required, especially for unencrypted connections, and the adversary could simply resume the session, possibly gaining privileged level access.

NSA recommends enabling TCP keep-alive settings for both inbound and outbound messages for all TCP connections with the following configuration commands:

```
service tcp-keepalives-in
service tcp-keepalives-out
```

Note that some devices do not support the configuration of TCP keep-alive messages.

7.7 Disable outbound connections

After authenticating to a device via a management port, a user generally has the ability to remotely connect to other systems on the network through supported protocols (e.g., Telnet and SSH). If an adversary was able to compromise the device or use an administrator account to gain user level access, this outbound connection could potentially be used to advance through the network. Properly reviewing device configurations and leveraging ACLs can prevent unauthorized systems from accessing network resources.

NSA recommends disabling outbound connections to limit an adversary from moving through the network with the following configuration commands:

```
line con 0
 transport output none

line vty 0 4
 transport output none

line vty 5 15
 transport output none
```

Depending on the device, it may be necessary to apply a similar configuration to other lines as well. If VTY lines 5 through 15 do not exist on a particular device, it is not necessary to execute those commands. It is critical to note that this feature must be explicitly disabled on the console line.

If outbound connections are required for copying files to or from the devices for maintenance or integrity verification, restrict it to only SSH and limit the number of devices that can be accessed via outbound ACLs; revert to the above configuration once the task is complete.

7.8 Remove SNMP read-write community strings

An SNMP version 1 or 2c read-write community string is similar to a password, and can be used to access or modify device configurations and operating system files. These actions generally cannot be done with a read-only community string. Because SNMP read-write community strings are sent in clear text, they can be exploited by an adversary to gain complete control of a network device.

NSA recommends removing all SNMP read-write community strings and upgrading to SNMP version 3 with encryption and authentication. If a version 1 or 2c SNMP read-write community string is required for remote administration and cannot be removed, it is recommended that the read-write community string be significantly different from other community strings to prevent an adversary from guessing the read-write community string if a read-only community string is obtained.

All version 1 and 2c SNMP community strings can be listed with the following exec command:

```
show running-config | include snmp-server community
```

Note: A read-write community string will include the `RW` keyword, while a read-only community string will include the `RO` keyword.

Disable an SNMP read-write community string with the following configuration command:

```
no snmp-server community <COMMUNITY_STRING>
```

7.9 Disable unnecessary network services

During the initial installation of devices, several TCP and UDP services are enabled by default, even though the provided features are unnecessary for normal operations. These services can degrade the security level of the network, offering an adversary additional access points to exploit a device and leave it susceptible to unauthorized monitoring, information gathering, and compromise.

For example, Cisco Smart Install is often unnecessary, but when left enabled, an unauthenticated remote adversary could use this service to obtain a device's configuration file, upload a new configuration or operating system image file, or force a reboot. This has been documented in Cisco's security advisory cisco-sa-20170214-smi as a misuse of the protocol, but the security community has observed and acknowledged this issue as a severe vulnerability exploited by adversaries to obtain configuration files across the Internet [38], [39].

NSA recommends disabling every unnecessary service on each device. If the service is required and can support a password and ACLs, create a password based on NSA's strong password guidance (see 5.5 Create strong passwords) and apply an ACL to only allow required systems to connect to the service. If a device does not support ACLs, it can be moved to a separate VLAN, and an ACL can be applied to the VLAN.

NSA also recommends immediately disabling the Cisco Smart Install service on all devices with the following configuration command:

```
no vstack
```

Even though this service is designed for switches, routers can also be configured as a Cisco Smart Install director; therefore, it should be explicitly disabled on all devices, especially when they are first configured.

Disable other unnecessary TCP and UDP services with the following configuration commands:

```
no service tcp-small-servers
no service udp-small-servers
no service finger
```

7.10 Disable discovery protocols on specific interfaces

Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) are broadcast protocols that periodically advertise network topology and device information to neighboring devices that support the protocol and are listening for packets. This functionality is enabled by default and can be useful for administrators to obtain information about the network, but it is also extremely useful to an adversary who can passively gather network configuration information. An adversary that is able to deploy a sniffer could collect device model numbers, operating system versions, VLAN information, and physical and logical addresses, gaining valuable information to exploit systems on the network.

NSA recommends disabling CDP and LLDP on all devices capable of using these services. If a service is required for proper network communications (e.g., some Cisco Voice-over-IP (VoIP) phones), only enable it on point-to-point links between devices that require the protocol or on voice enabled ports.

CDP and LLDP can be globally disabled with the following configuration commands:

```
no cdp run
no lldp run
```

If CDP is required on specific interfaces, it must be globally enabled but disabled on all other interfaces, as shown in the following configuration commands for a single interface:

```
interface <INTERFACE>
 no cdp enable
```

7.11 Configure remote network administration services

This section describes how to properly enable common remote network administration services.

7.11.1 Configuring SSH for remote administration

Allow inbound SSH connections with the following configuration commands:

```
line vty 0 4
 transport input ssh
```

```
line vty 5 15
 transport input ssh
```

Note: This may disable other services enabled on the lines by default, such as Telnet. If VTY lines 5 through 15 do not exist on a particular device, it is not necessary to execute those commands. Depending on the device, it may be necessary to apply a similar configuration to other lines as well.

Allowed input transports can be confirmed with the following exec command:

```
show line <LINE> <LINE_NUMBER>
```

Disable SSH version 1 connections and only allow version 2 of the protocol with the following configuration command:

```
ip ssh version 2
```

Generate a new asymmetric Rivest-Shamir-Adleman (RSA) key pair for SSH with the following configuration command:

```
crypto key generate rsa modulus 3072
```

Note: This command will overwrite an existing RSA key pair.

Generate a new asymmetric ECC key pair for SSH with the following configuration command:

```
crypto key generate ec keysize 384
```

Note: This command will overwrite an existing ECC key pair.

Set the minimum Diffie-Hellman key size to 4096 bits with the following configuration command:

```
ip ssh dh min 4096
```

Note: Some devices do not support 3072 bits for the Diffie-Hellman key size, so 4096 bits is recommended.

The encryption, key exchange (KEX), and message authentication code algorithms accepted by the SSH protocol can be specified (to include the preferred order) with the following configuration commands:

```
ip ssh server algorithm encryption <ALGORITHM> [<ALGORITHM> ...]
ip ssh server algorithm kex <ALGORITHM> [<ALGORITHM> ...]
ip ssh server algorithm mac <ALGORITHM> [<ALGORITHM> ...]
```

For more information on acceptable algorithms, refer to CNSSP 15 [4]. The CNSSP 15 requirements are explained in the draft IETF document on Commercial National Security Algorithm (CNSA) Suite Cryptography for Secure Shell (SSH) [36].

The configuration of the SSH service can be confirmed with the following exec command:

```
show ip ssh
```

Apply a standard ACL to only permit IP addresses used by administrators with the following configuration commands:

```
line vty 0 4
 access-class <ACL#> in

line vty 5 15
 access-class <ACL#> in
```

If VTY lines 5 through 15 do not exist on a particular device, it is not necessary to execute those commands. Note that this ACL would also apply to Telnet if it was enabled on the lines. Depending on the device, it may be necessary to apply a similar configuration to other lines as well. Refer to 7.4 Limit access to services for more information on creating a standard ACL.

Set the session expiration to 5 minutes or less with the following configuration commands:

```
line con 0
 exec-timeout 5 0

line vty 0 4
 exec-timeout 5 0
```

```
line vty 5 15
 exec-timeout 5 0
```

If VTY lines 5 through 15 do not exist on a particular device, it is not necessary to execute those commands.

Note: This would also apply to Telnet if it was enabled on the lines. Depending on the device, it may be necessary to apply a similar configuration to other lines as well.

7.11.2 Configuring HTTP for remote administration

If HTTP is used for management purposes, enable HTTP over TLS with the following configuration command:

```
ip http secure-server
```

Only accept TLS version 1.2 with the following configuration command:

```
ip http tls-version TLSv1.2
```

The cipher suites accepted by the encrypted HTTP service can be specified (to include the preferred order) with the following configuration command:

```
ip http secure-ciphersuite <CIPHERSUITE> [<CIPHERSUITE> ...]
```

For more information on acceptable algorithms, refer to CNSSP 15 [4]. The CNSSP 15 requirements are explained in the draft IETF document on Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3 [35].

Apply a standard ACL to only permit IP addresses used by administrators with the following configuration command:

```
ip http access-class <ACL#>
```

Note: This ACL would also apply to the clear text HTTP service if it was enabled. For more information on creating a standard ACL, refer to 7.4 Limit access to services.

The default idle timeout of an HTTP server connection is 180 seconds (three minutes), so it is not necessary to change this value.

7.11.3 Configuring SNMP for remote administration

If SNMP is used for management, enable SNMP version 3 with both authentication and privacy (encryption) with the following configuration commands:

```
snmp-server group <SNMPv3_GROUP> v3 priv access <ACL#>
snmp-server user <USER> <SNMPv3_GROUP> v3 auth sha <AUTH_PASSWORD> priv aes
 256 <PRIV_PASSWORD> access <ACL#>
```

First a group must be defined, where the `priv` keyword is equivalent to authPriv (both authentication and privacy). One or more users must be defined and assigned to a group. In addition to the authentication and encryption parameters, two different passwords must be supplied for each user, one for authentication and one for privacy. Interoperability issues have been observed with AES-192 and AES-256, so it may be necessary to use AES-128 for encryption instead of AES-256 with the `aes 128` keywords. As shown above, an ACL can be applied to both the group and each individual user by specifying it as a separate option at the end of each command with the `access` keyword.

The above SNMP configuration can be tested from a Linux system with the following shell command:

```
snmpget -v 3 -u <USER> -a sha -l authPriv -A '<AUTH_PASSWORD>' -x AES \
 -X '<PRIV_PASSWORD>' <IP_ADDRESS> 1.3.6.1.2.1.1.5.0
```

Return to Contents

8. Routing

Routers forward data packets between computer networks. When a router receives a packet, it uses its routing table and the packet's network address information to determine the next hop to reach its destination. An improper configuration of the router itself or the dynamic routing protocols used to populate the routing table could allow an adversary to redirect packets to a different destination, allowing sensitive data to be collected, manipulated, or discarded, which would violate confidentiality, integrity, or availability.

Configure your routers for network use vs. malicious abuse.

8.1 Disable IP source routing

IP source routing is a rarely used feature that enables the sender of a packet to specify a pre-determined list of intermediate nodes where it should be forwarded rather than using the internal routing table to make a decision. Leveraging this setting, an adversary could transmit packets through a route of their choosing. Along with IP address spoofing, an adversary can use the IP source routing feature to successfully bypass ACLs and other network restrictions, essentially choosing its own network path. Although this vulnerability is associated with routers and how packets are routed, the functionality can also be exploited on switches.

NSA recommends disabling IP source routing on all devices, not just routers, since this feature is not required for normal network operations. Depending on the vendor of a product, it may be necessary to disable forwarding of each IP source route option individually. A similar feature is available in IPv6, and needs to be disabled separately. Disable IP source routing with the following configuration commands:

```
no ip source-route
no ipv6 source-route
```

8.2 Enable unicast reverse-path forwarding (uRPF)

uRPF is a method of protection against IP spoofing that instructs a router to examine both the source and destination addresses in the packet. When a packet is received on an interface, the source address is compared to entries in the routing table and is forwarded if the return route matches where the packet was received. Otherwise, it is discarded due to concerns that the source address in the packet may have been spoofed. If uRPF is not enabled, an adversary may be able to successfully spoof the source address of IP packets sent into the network.

NSA recommends enabling uRPF on external interfaces of perimeter routers. On routers, it is necessary for Cisco Express Forwarding (CEF), which provides optimized lookups for efficient packet forwarding, to be enabled before uRPF. Note that uRPF should not be enabled on internal interfaces or routers that have asymmetrical routing (where two or more return routes may exist for a given source address), as this situation could cause legitimate packets to be discarded. Enable uRPF on a single interface with the following configuration commands:

```
ip cef
interface <INTERFACE>
 ip verify unicast reverse-path
```

8.3 Enable routing authentication

Dynamic routing protocols are used to distribute information to neighboring devices and provide routes to reach other networks. Network devices will use this information to populate their routing tables, which are then used to determine the next hop for forwarding a packet to the requested destination. To control the flow of traffic, an adversary may inject, modify, or corrupt the routing information sent and received by neighboring devices. Routing authentication should be enabled to prevent route manipulation and ensure the routing information received from neighboring devices has not been manipulated by an unauthorized source.

NSA recommends enabling routing authentication on any dynamic routing protocols used that receive routing updates from other devices on the network. Enable Open Shortest Path First (OSPF) routing authentication by enabling it on the OSPF process for each area and applying the authentication key to each interface associated with that process with the following configuration commands:

```
key chain <KEY_CHAIN_NAME>
 key <KEY_NUMBER>
 key-string <KEY>
 cryptographic-algorithm hmac-sha-512

interface <INTERFACE>
 ip ospf authentication key-chain <KEY_CHAIN_NAME>
```

NSA also recommends using a unique key between all neighbors, instead of using the same authentication key for all interfaces on all devices. If the keys are different, an adversary would not be able to use a compromised key from one network to inject a malicious route on another network.

Enable Border Gateway Protocol (BGP) routing authentication by applying a unique password key to each individual peer with the following configuration commands:

```
router bgp <AS_NUMBER>
 peer <IP_ADDRESS_1> password <KEY>
```

Enable Enhanced Interior Gateway Routing Protocol (EIGRP) authentication by creating a key-chain and applying it to each interface with the following configuration commands:

```
key chain <KEY_CHAIN_NAME>
 key <KEY_NUMBER>
  key-string <KEY>
  cryptographic-algorithm hmac-sha-512

interface <INTERFACE>
 ip authentication key-chain eigrp <AS_NUMBER> <KEY_CHAIN_NAME>
```

Note: An arbitrary name and number can be chosen for each key. The *<KEY>* is the shared key assigned to neighboring devices. The `cryptographic-algorithm` can also be set to `hmac-sha-384` and still meet CNSSP 15 guidance [4].

Do not use the Routing Information Protocol (RIP). It is slow to converge, does not scale, and RIP version 1 cannot be configured to authenticate nearby routers, making it easy for an adversary to exploit the protocol. Devices that only support RIP should use static or default routes to other devices that support modern routing protocols with authentication.

Return to Contents

9. Interface ports

The interface ports of network switches physically connect workstations, servers, and other devices to the network, while the interconnections between routers and switches define how systems communicate across the network. An adversary must first obtain physical access to the network to connect an unauthorized system, or use an authorized system already on the network to exploit an existing connection. Properly configured interface ports can prevent an adversary from performing exploitation attempts against the network.

Prevent an adversary from connecting to your network.

9.1 Disable dynamic trunking

A trunk is a point-to-point link between two devices that exchange VLAN encapsulated frames. Depending on the traffic being sent over the link, it is possible for an interface

port to dynamically configure itself to be either a trunk or an access port. An adversary that is connected to a dynamic port could instruct it to become a trunk port and potentially gain access to network traffic without regard to VLAN separation.

NSA recommends disabling dynamic trunking as it is not necessary for an interface port to dynamically configure itself. When a device is added to the network, ensure that all interface ports are explicitly configured as either trunk ports or access ports. Systems that do not handle VLAN encapsulated frames should be connected to a port that is configured for access only.

Strictly configure an interface port for static access only with the following configuration commands:

```
interface <INTERFACE>
 switchport mode access
```

Strictly configure an interface port to be a trunk with the following configuration commands:

```
interface <INTERFACE>
 switchport mode trunk
```

9.2 Enable port security

Physical interface ports of devices are often the primary means of restricting physical access to a network. Port security limits the number of valid MAC addresses allowed to connect to a switchport, restricting connectivity to only authorized systems. A switchport not configured to enforce port security could allow an adversary with physical access to connect an unauthorized system. The adversary could bypass existing security restrictions, gather network information, probe deeper into the network, or compromise internal systems.

NSA recommends enabling port security on all active switchports on a device, and setting the maximum number of allowed MAC addresses for each port to be exactly one, or two if VoIP capabilities are in use. Port security is not a replacement for a NAC, such as 802.1X, but should be used when a NAC cannot be implemented. If possible, assign a fixed MAC address to each switchport that is connected to a known system, and configure each switchport to either shutdown or send an SNMP trap message when a port security violation occurs. Port security can be enabled on trunk interfaces;

however, it is not recommended as it requires knowing the number of devices that have traffic traversing that specific trunk. A dynamic switchport cannot have port security enabled simultaneously, and must first be configured for static access before port security can be enabled.

Enable port security on a static access port with a maximum of one MAC address with the following configuration commands:

```
interface <INTERFACE>
 switchport mode access
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation shutdown
 switchport port-security mac-address sticky
```

The `sticky` keyword will allow the device to insert the MAC address in the configuration once the first authorized system is connected to that port.

Note: The configuration will need to be saved to retain the information after a reboot. If shutting down a port is not an acceptable action because of availability concerns, the `shutdown` keyword can be replaced with `restrict` to prevent any additional MAC addresses from communicating on that port.

9.3 Disable default VLAN

Most switches utilize VLAN 1 as the default, including management ports, which may provide direct access to the switch for administration. Additionally, some layer 2 protocols (e.g., discovery or trunking) need to be sent on a specific VLAN on trunk links, and VLAN 1 is generally selected as the default. If mitigation steps are not taken, the default VLAN may span the entire network, and place authorized systems at a higher risk of exploitation by unauthorized systems that gain access.

NSA recommends moving all management and operational traffic to different VLANs (not the default) that separate management traffic from user data and protocol traffic, and using multiple switches to separate different security levels of network traffic. The default VLAN should also be logically disallowed on all trunks and access ports that don't require it (including disconnected and shutdown ports) to ensure it does not transmit unnecessary broadcast, multicast, and unknown destination traffic.

Frames that are sent and received on trunk ports are usually tagged with the VLAN ID associated with the frame. Any frames received that are not tagged are automatically placed in the native trunking VLAN associated with that port. The native trunking VLAN should be assigned the same on both ends of a trunk link. Similarly, frames that are sent and received on access ports are assigned to the access VLAN associated with that port. All switchports are assigned to an access VLAN and a native trunking VLAN, regardless if they are trunk or access ports.

NSA recommends assigning all trunk ports to a unique native trunking VLAN that is only assigned to trunk ports, and assigning the access VLAN to an unused and disabled VLAN. Similarly, NSA recommends assigning all access ports to the appropriate access VLAN, and assigning the native trunking VLAN to another unused and disabled VLAN, different from the ones used by trunk ports. This configuration will prevent an adversary from jumping between active VLANs by intentionally tagging traffic that would otherwise be untagged.

Create a unique trunking VLAN (500) and an unused and disabled access VLAN (997), both assigned to a trunk port, with the following example configuration commands:

```
vlan 500
 name NATIVE-TRUNK

vlan 997
 name UNUSED-ACCESS
 shutdown

interface <INTERFACE>
 switchport mode trunk
 switchport access vlan 997
 switchport trunk native vlan 500
 switchport trunk allowed vlan 2-4094
```

This configuration also allows all VLANs, except for the default VLAN 1, to traverse the trunk. If all configured VLANs are known, NSA recommends allowing only those specific VLANs, rather than just excluding VLAN 1.

Create an unused and disabled VLAN (998), assigned to the native trunking VLAN of an access port, with the following example configuration commands:

```
vlan 998
 name UNUSED-NATIVE
 shutdown

interface <INTERFACE>
 switchport mode access
 switchport access vlan <ACCESS_VLAN#>
 switchport trunk native vlan 998
```

Switchports can also be assigned a third VLAN, if VoIP capabilities are in use, with the following configuration commands:

```
interface <INTERFACE>
 switchport voice vlan <VOICE_VLAN#>
```

All of the VLANs associated with individual switchports can be confirmed with the following exec command:

```
show interfaces switchport
```

9.4 Disable unused ports

Leaving unused ports enabled on a device allows an adversary to attach a rogue device to the network and perform information gathering or compromise attempts. All unused ports should be disabled and placed in an unused VLAN, which is not the default.

NSA recommends disabling all unused ports on a device by shutting down the associated interfaces and, if supported by the device, assigning unused ports to an unused VLAN. This will continue to prevent access to the network, even if the ports become enabled. Prior to disabling a port, it is necessary to verify that it is truly unused and nothing is connected. If a device connected to the port is powered off, it may appear that the switchport is unused.

Shut down all unused interfaces and assign the access and native trunking VLANs to unused and disabled VLANs with the following example configuration commands:

```
vlan 999
 name UNUSED-DISABLED
 shutdown

interface <INTERFACE>
 switchport mode access
 switchport access vlan 999
```

```
switchport trunk native vlan 998
no switchport voice vlan
shutdown
```

Note: It is not necessary to assign the voice VLAN to an unused VLAN, as it will remain unassigned if VoIP capabilities are not in use.

9.5 Disable port monitoring

Port monitoring is used on a network switch to send a copy of network packets seen on one switchport to a network monitoring connection on another switchport. A device that has one or more port monitoring sessions defined allows a set of source ports to be monitored by a specified destination port, and all traffic being sent to or from the source ports will also be sent to the destination port.

Port monitoring is typically used for connecting an NIDS, diagnosing a problem, or using a network analyzer to monitor the network. Depending on the vendor, port monitoring is also known as “port mirroring” or “port spanning.” An adversary connected to the destination port of a port monitoring session will be able to collect network traffic sent through all the source ports specified by the session.

NSA recommends disabling all inactive port monitoring sessions on a device. Port monitoring should only be enabled for those ports where it is necessary, and all sessions should be disabled once they are no longer needed.

Note: Some vendors do not allow traffic to be sent from the destination port of a port monitoring session, effectively disabling network access from that port. This type of behavior is desired when a NIDS is connected to a port monitoring session.

List the monitoring sessions defined in the configuration with the following exec command:

```
show monitor session [1|2|all]
```

Note: If the `all` keyword is supported, it will list all of the defined sessions; otherwise each individual session number will need to be specified in separate commands, generally `1` and `2`.

Remove a monitoring session defined in the configuration with the following configuration command:

```
no monitor session <SESSION#>
```

9.6 Disable proxy Address Resolution Protocol (ARP)

Proxy ARP is a technique in which a proxy server on a network answers ARP requests for an IP address that is not on that network. It helps devices on a subnet reach remote subnets, without configuring routing on a default gateway. It can be advantageous since it can be added to a router without disbursing routing tables from other networks, but this feature allows adversaries to spoof a system and intercept packets.

NSA recommends disabling proxy ARP on all interfaces unless the device is being used as a LAN bridge or to allow inbound network address translations (NAT) for multiple destination IP addresses. It may be necessary to disable proxy ARP on each individual interface, rather than disabling it globally.

Find interfaces that have proxy ARP enabled with the following exec command:

```
show ip interface
```

Disable Proxy ARP on an individual interface with the following configuration commands:

```
interface <INTERFACE>
 no ip proxy-arp
```

Return to Contents

10. Notification and consent banners

The technical recommendations provided in this guide can significantly reduce the probability of an adversary exploiting a vulnerability on the network. Unfortunately, an adversary or insider may still find a weakness to compromise, circumvent, or disrupt the network. Having a notification banner can make clear what is permissible to anyone who accesses the system, and add any necessary notices and disclaimers.

Display notifications of authorized use and consent to monitoring.

10.1 Present a notification banner

Depending on the organization's requirements, a notification banner can provide notice to users that connecting to the network device is for authorized use only and that any use of the system is subject to monitoring for any authorized purpose. A legally sufficient banner ensures the network owner and others, including the Government, can take necessary steps to monitor and secure the network. However, the precise requirements for such a banner will vary by organization and jurisdiction.

For example, DoD elements must use a banner that meets the requirements of DoD Instruction 8500.01. Other U.S. Government entities should implement the requirements of NIST SP800-53, AC-8. For private sector entities, the Cybersecurity and Infrastructure Security Agency has issued very helpful guidance on developing an appropriate banner [40].

NSA recommends that each device be configured to present the full notification banner whenever a user logs into an information system or connects to any remote service.

Cisco IOS devices have two types of banners; the login banner is displayed prior to a user logging in, and then the "message of the day" is displayed after the user successfully authenticates. At a minimum, the notification banner should be displayed to both authorized and unauthorized users attempting to login. The same or additional information could be provided to authenticated users after logging in, if desired.

Add a notification banner, with the organization's banner appropriately inserted, prior to users logging in with the following configuration command:

```
banner login ^
INSERT NOTIFICATION BANNER HERE
^
```

Note: The caret symbol (“^”) is used as a delimiter so the banner can span multiple lines, assuming the caret symbol is not used in the banner itself. After this command is inserted into the configuration, the delimiter will generally appear as “^C” instead of “^”. Do not type in “^C” as part of the command, otherwise the banner will begin with a “C”.

Add the same notification banner or additional information for authorized users who have successfully authenticated with the following configuration command:

```
banner motd ^
INSERT NOTIFICATION BANNER HERE
ADDITIONAL INFORMATION
^
```

Return to Contents

11. Conclusion

The guidance in this report was generated from a depth and breadth of experience in assisting NSA customers with evaluating their networks and providing recommendations to immediately harden network devices. Along with essential maintenance functions, administrators play a critical role in defending networks against adversarial threats. Following this guide will assist these network defenders with implementing cybersecurity best practices, lowering the risk against compromise and ensuring a more secure and better-protected network.

Abbreviations

AAA	Authentication, authorization, and accounting
ACL	Access control list
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
AUX	Auxiliary
BGP	Border Gateway Protocol
CDP	Cisco Discovery Protocol
CEF	Cisco Express Forwarding
CISA	Cybersecurity and Infrastructure Security Agency
CNSA	Commercial National Security Algorithm Suite
CNSSP	Committee on National Security Systems Policy
CON	Console
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized zone
DoS	Denial of service
ECC	Elliptic curve cryptography
ECP	Elliptic curve group modulo a prime
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IOS	Internetwork Operating System
IP	Internet Protocol
IPS	Intrusion prevention system
IPsec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet service provider
KEX	Key exchange
LAN	Local area network
LLDP	Link Layer Discovery Protocol
MAC	Media access control
MD5	Message Digest 5
MODP	Modular Exponent
NAC	Network access control
NAT	Network address translation
NDI	Network Device Integrity
NIDS	Network intrusion detection system
NIST	National Institute of Standards and Technology
NSA	National Security Agency

NSS	National Security System(s)
NTP	Network Time Protocol
OMB	Office of Management and Budget
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
RSA	Rivest-Shamir-Adleman
SCP	Secure Copy Protocol
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIEM	Security information and event management
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
uRPF	Unicast reverse-path forwarding
UTC	Coordinated Universal Time
VLAN	Virtual local area network
VoIP	Voice over IP
VPN	Virtual private network
VTY	Virtual teletype

References

Works cited

[1] Cybersecurity and Infrastructure Security Agency (2022), Layering Network Security Through Segmentation. Available at: https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf

[2] National Security Agency (2019), Segment Networks and Deploy Application-aware Defenses. Available at: https://www.nsa.gov/cybersecurity-guidance

[3] National Security Agency (2021), Selecting and Hardening Remote Access VPN Solutions. Available at: https://www.nsa.gov/cybersecurity-guidance

[4] Committee on National Security Systems (2016), CNSS Policy 15. Available at: https://www.cnss.gov/CNSS/issuances/Policies.cfm

[5] Corcoran, Jenkins, NSA (2021), Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec). Available at: https://datatracker.ietf.org/doc/html/draft-corcoran-cnsa-ipsec-profile

[6] National Security Agency (2020), Configuring IPsec Virtual Private Networks. Available at: https://www.nsa.gov/cybersecurity-guidance

[7] National Security Agency (2019), Mitigating Recent VPN Vulnerabilities. Available at: https://www.nsa.gov/cybersecurity-guidance

[8] National Security Agency (2021), Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations. Available at: https://www.nsa.gov/cybersecurity-guidance

[9] Arista Networks, Inc. (2022), Support Overview. Available at: https://www.arista.com/en/support/

[10] Aruba Networks (2022), Aruba Support Services. Available at: https://www.arubanetworks.com/support-services/

[11] Broadcom Inc. (2022), Support and Services. Available at: https://www.broadcom.com/support/

[12] Cisco Systems, Inc. (2022), Support & Downloads. Available at: https://www.cisco.com/c/en/us/support/index.html

[13] Dell (2022), Support. Available at: https://www.dell.com/support/home/en-us/

[14] Extreme Networks (2022), Support. Available at: https://www.extremenetworks.com/support/

[15] F5, Inc. (2022), Support | Services. Available at: https://www.f5.com/services/support/

[16] Fortinet, Inc. (2022), FortiCare Technical Support and Services. Available at: https://www.fortinet.com/support

[17] Hewlett Packard Enterprise Development LP (2022), Services and Support. Available at: https://www.hpe.com/us/en/services.html

[18] International Business Machines Corporation (2022), IBM Support. Available at: https://www.ibm.com/mysupport/

[19] Juniper Networks, Inc. (2022), Support. Available at: https://support.juniper.net/support/

[20] Linksys Holdings (2022), Official Linksys Support Site. Available at: https://www.linksys.com/us/support/

[21] NETGEAR (2022), Support. Available at: https://www.netgear.com/support/

[22] Palo Alto Networks (2022), Customer Support. Available at: https://support.paloaltonetworks.com/support/

[23] Riverbed Technology (2022), Riverbed Support. Available at: https://support.riverbed.com/
[24] CommScope, Inc. (2022), Ruckus Wireless Support. Available at: https://support.ruckuswireless.com/
[25] SonicWall (2022), Support Portal & Downloads. Available at: https://www.sonicwall.com/support/
[26] TRENDnet Inc. (2022), Customer Support. Available at: https://www.trendnet.com/support/
[27] Eaton (2022), Help Center | Tripp Lite. Available at: https://www.tripplite.com/support/
[28] Ubiquiti Inc. (2022), Ubiquiti Support and Help Center. Available at: https://help.ui.com/hc/en-us/
[29] WatchGuard Technologies, Inc. (2022), WatchGuard Support. Available at: https://www.watchguard.com/wgrd-support/overview
[30] National Security Agency (2016), Network Device Integrity (NDI) Methodology. Available at: https://media.defense.gov/2023/Oct/06/2003315573/-1/-1/0/NETWORK%20DEVICE%20INTEGRITY%20NDI%20METHODOLOGY.PDF
[31] National Security Agency (2016), Network Device Integrity (NDI) on Cisco IOS devices. Available at: https://media.defense.gov/2023/Oct/06/2003315572/-1/-1/0/NETWORK%20DEVICE%20INTEGRITY%20ON%20CISCO%20IOS%20DEVICES.PDF
[32] National Security Agency (2016), Validate Integrity of Hardware and Software. Available at: https://media.defense.gov/2023/Oct/06/2003315571/-1/-1/0/VALIDATE%20INTEGRITY%20OF%20HARDWARE%20AND%20SOFTWARE.PDF
[33] National Security Agency (2022), Cisco Password Types: Best Practices. Available at: https://www.nsa.gov/cybersecurity-guidance
[34] Office of Management and Budget (2021), Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents. Available at: https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf
[35] Cooley, D, NSA (2021), Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3. Available at: https://datatracker.ietf.org/doc/html/draft-cooley-cnsa-dtls-tlsprofile
[36] Gajcowski, Jenkins, NSA (2021), Commercial National Security Algorithm (CNSA) Suite Cryptography for Secure Shell (SSH). Available at: https://datatracker.ietf.org/doc/html/draft-gajcowski-cnsa-ssh-profile
[37] National Institute for Standards and Technology (2020), Special Publication 800-52 Rev. 2: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. Available at: https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
[38] Cisco Systems, Inc. (2017), Cisco Smart Install Protocol Misuse. Available at: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi
[39] National Security Agency (2017), Cisco Smart Install Protocol Misuse. Available at: https://www.nsa.gov/cybersecurity-guidance
[40] Cybersecurity and Infrastructure Security Agency (2022), Guidance on Consent Banners. Available at: https://www.cisa.gov/publication/guidance-consent-banners

Related guidance

- Biden (2021), Executive Order 14028: Improving the Nation's Cybersecurity. Available at: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
- National Institute of Standards and Technology (2020), Special Publication 800-207: Zero Trust Architecture. Available at: https://www.nist.gov/publications/zero-trust-architecture
- Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team (2021), Department of Defense (DOD) Zero Trust Reference Architecture. Available at: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf
- National Institute for Standards and Technology (2020), Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management. Available at: https://pages.nist.gov/800-63-3/sp800-63b.html
- National Security Agency (2019), Continuously Hunt for Network Intrusions. Available at: https://www.nsa.gov/cybersecurity-guidance
- National Security Agency (2021), Embracing a Zero Trust Security Model. Available at: https://www.nsa.gov/cybersecurity-guidance
- National Security Agency (2020), Hardening Network Devices. Available at: https://www.nsa.gov/cybersecurity-guidance

SecureCloud Solutions

Confidential Internal Document

Cybersecurity Posture Overview

Date: June 15, 2023

1. Executive Summary

SecureCloud Solutions is committed to maintaining the highest standards of cybersecurity to protect our clients' data and our internal systems. This document provides an overview of our current cybersecurity posture, highlighting our strengths and areas for continuous improvement.

2. Network Security

2.1 Perimeter Defense

- Implemented Palo Alto Networks PA-5250 next-generation firewalls
- Cisco Firepower 4110 NGIPS for intrusion prevention
- Imperva WAF for web application protection

2.2 Network Segmentation

- Implemented micro-segmentation using VMware NSX
- Critical assets isolated in separate VLANs
- Zero Trust Network Access (ZTNA) principles applied

2.3 Remote Access

- Cisco AnyConnect Secure Mobility Client for VPN access
- Split-tunnel VPN configuration to optimize performance

3. Data Protection

3.1 Encryption

- AES-256 encryption for data at rest

- TLS 1.3 for data in transit
- Gemalto SafeNet KeySecure for key management

3.2 Data Loss Prevention
- Symantec DLP suite implemented across endpoints and network
- Regular DLP policy reviews and updates

3.3 Access Control
- Implemented Okta for Identity and Access Management (IAM)
- Role-Based Access Control (RBAC) enforced across all systems
- Quarterly access reviews conducted

4. Incident Response

4.1 IR Plan
- Comprehensive IR plan documented and updated bi-annually
- Clearly defined roles and responsibilities for IR team members

4.2 Detection and Analysis
- Splunk SIEM for log aggregation and analysis
- IBM QRadar for advanced threat detection

4.3 Containment and Eradication
- Automated containment procedures for critical systems
- Partnerships with forensic analysis firms for complex incidents

4.4 Testing and Improvement
- Quarterly tabletop exercises
- Annual full-scale IR simulation

5. Compliance

5.1 Regulatory Compliance

- SOC 2 Type II certified
- GDPR and CCPA compliant
- HIPAA compliance for healthcare clients

5.2 Compliance Monitoring

- Implemented OneTrust for compliance management
- Automated compliance checks using Qualys Policy Compliance

5.3 Audits and Assessments

- Annual third-party penetration testing
- Quarterly internal security audits

6. Endpoint Security

6.1 Endpoint Protection

- CrowdStrike Falcon deployed on all endpoints
- Carbon Black EDR for advanced threat hunting

6.2 Patch Management

- Automated patch management using Ivanti Security Controls
- Critical patches applied within 24 hours of release

6.3 Mobile Device Management

- VMware Workspace ONE for MDM and MAM
- Strict BYOD policies enforced

7. Authentication

7.1 Multi-Factor Authentication

- Duo Security MFA implemented across all systems
- Hardware security keys (YubiKey) for privileged accounts

7.2 Password Policies
- Minimum 16-character passwords with complexity requirements
- Password rotation every 90 days
- Password managers provided to all employees

7.3 Advanced Authentication
- Piloting FIDO2 passwordless authentication

8. Cloud Security

8.1 Cloud Service Providers
- Utilizing AWS and Azure with their respective native security tools
- Regular security configuration reviews using CloudCheckr

8.2 Cloud Access Security
- Implemented Netskope CASB solution
- Data classification and tagging for all cloud-stored data

8.3 Containerization Security
- Aqua Security for container and Kubernetes security
- Twistlock for runtime protection of containers

9. Security Awareness

9.1 Training Program
- KnowBe4 platform for security awareness training
- Mandatory quarterly training sessions for all employees

9.2 Phishing Simulations

- Monthly phishing tests with targeted training for failures

- Phish alert button installed on all email clients

9. 3 Security Champions

- Designated security champions in each department

- Quarterly security awareness newsletters

10. Conclusion

SecureCloud Solutions is committed to maintaining a robust cybersecurity posture. This document highlights our current security controls and areas for improvement. We will continue to invest in our security infrastructure and employee training to stay ahead of emerging threats.