GDPR checklist

Use this checklist to assess your GDPR audit readiness and implementation status.

Want to improve your score and compliance? Let CyberArrow do it for you. Schedule a live demo

Control ID	Control Name	Control Description	Implementation Status
2.2	Material Scope	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. This Regulation does not apply to the processing of personal data: a) in the course of an activity which falls outside the scope of Union law; b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; c) by a natural person in the course of a purely personal or household activity; d) 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. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. 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. 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.	Not Implemented
2.3	Territorial scope	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. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not	Not Implemented

		established in the Union, where the processing activities are related to: a) 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 b) the monitoring of their behaviour as far as their behaviour takes place within the Union. 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.	
2.5.1	Principles relating to processing of personal data - Data Processing	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);	Not Implemented
2.5.2	Principles relating to processing of personal data - Data Collection	Personal data shall be 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(a), not be considered to be incompatible with the initial purposes (‘purpose limitation’);	Not Implemented
2.5.3	Principles relating to processing of personal data - Data Minimization	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimization’);	Not Implemented
2.5.4	Principles relating to processing of personal data - Accuracy	Personal data shall be 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’);	Not Implemented
2.5.5	Principles relating to processing of personal data - Data Storage	Personal data shall be 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(a) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order	Not Implemented

		to safeguard the rights and freedoms of the data subject ('storage limitation');	
2.5.6	Principles relating to processing of personal data - Integrity and confidentiality	Personal data shall be 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').	Not Implemented
2.5.7	Principles relating to processing of personal data - Data Controller's Responsibility	The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').	Not Implemented
2.6.1	Lawfulness of processing - Processing	Processing shall be lawful only if and to the extent that at least one of the following applies: a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; b) 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; c) processing is necessary for compliance with a legal obligation to which the controller is subject; d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; e) 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; f) 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. * The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (f) 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. * That legal	Not Implemented

		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.	
2.6.4	Lawfulness of processing - Purpose of the processing	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(a), 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: a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; c) 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; d) the possible consequences of the intended further processing for data subjects; e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.	Not Implemented
2.7.1	Conditions for consent - Evidence of the provided consent	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.	Not Implemented

2.7.2	Conditions for consent - Documenting the Consent	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. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.	Not Implemented
2.7.3	Conditions for consent - Consent Withdrawal	The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed therof. It shall be as easy to withdraw as to give consent.	Not Implemented
2.7.4	Conditions for consent - Assessing whether consent is freely given	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.	Not Implemented
2.8	Conditions applicable to child's consent in relation to information society services	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. 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. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years. 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. 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.	Not Implemented

2.9	Processing of special categories of personal data	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. Paragraph 1 shall not apply if one of the following applies: a) 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; b) 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; c) 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; d) 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; e) processing relates to personal data which are manifestly made public by the data subject; f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; g) processing is necessary for reasons of substantial public interest, on the	Not Implemented

		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; h) 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; i) 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; j) 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. 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. Member States may maintain or introduce further conditions,	

		including limitations, with regard to the processing of genetic data, biometric data or data concerning health.	
2.11	Processing which does not require identification	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. 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. 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.	Not Implemented
3.12.1	Transparent information, communication and modalities for the exercise of the rights of the data subject	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. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. 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.	Not Implemented

3.12.2	The rights of the data subject - Data Subjects Rights	The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. 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.	Not Implemented
3.12.3	The rights of the data subject - Notifying data subject about action taken	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. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. 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. 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.	Not Implemented
3.12.4	The rights of the data subject - Notifying data subject about action not taken	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.	Not Implemented
3.12.5	The rights of the data subject - Charges	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. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	Not Implemented

3.12.6	The rights of the data subject - Request for additional information	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.	Not Implemented
3.13.1	Information to be provided where personal data are collected from the data subject	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: a) the identity and the contact details of the controller and, where applicable, of the controller's representative; b) the contact details of the data protection officer, where applicable; c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; e) the recipients or categories of recipients of the personal data, if any; f) 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.	Not Implemented
3.13.2	Information to be provided - Fair and transparent processing	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: a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; b) 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; c) where the processing is based on	Not Implemented

		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; d) the right to lodge a complaint with a supervisory authority; e) 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; f) 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.	
3.13.3	Information to be provided - Further processing requirement	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.	Not Implemented
3.13.4	Information to be provided - Exceptions	Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.	Not Implemented
3.14.1	Information to be provided - Controller Information	Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: a) the identity and the contact details of the controller and, where applicable, of the controller's representative; b) the contact details of the data protection officer, where applicable; c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; d) the categories of personal data concerned; e) the recipients or categories of recipients of the personal data, if any; f) 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	Not Implemented

		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.	
3.14.2	Information to be provided - Additional requirements for transparent data processing	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: a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; c) 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; d) 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; e) the right to lodge a complaint with a supervisory authority; f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources; g) 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.	Not Implemented
3.14.3	Information to be provided - Communication Timeframe	The controller shall provide the information referred to in paragraphs 1 and 2: a) 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; b) 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 c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.	Not Implemented

3.14.4	Information to be provided - Further processing requirements	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.	Not Implemented
3.14.5	Information to be provided by Controller - Exceptions	Paragraphs 1 to 4 shall not apply where and insofar as: a) the data subject already has the information; b) 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; c) 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 d) 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.	Not Implemented
3.15.1	Right of access by the data subject - Confirmation for processing data	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: a) the purposes of the processing; b) the categories of personal data concerned; c) 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; d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that	Not Implemented

		period; e) 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; f) the right to lodge a complaint with a supervisory authority; g) where the personal data are not collected from the data subject, any available information as to their source; h) 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.	
3.15.2	Right of access by the data subject - Rules for transferring data to a third country or international organization	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.	Not Implemented
3.15.3	Right of access by the data subject - Copy of the data processing	The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. 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.	Not Implemented
3.16	Right to rectification	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. 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.	Not Implemented
3.17.1	Right to erasure (right to be forgotten) - Rules for data erasure	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: a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; b) the data	Not Implemented

		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; c) 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); d) the personal data have been unlawfully processed; e) 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; f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).	
3.17.2	Right to erasure (right to be forgotten) - Erasure of publicly available data	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.	Not Implemented
3.17.3	Right to erasure (right to be forgotten) - Exceptions	Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: a) for exercising the right of freedom of expression and information; b) 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 c) interest or in the exercise of official authority vested in the controller; d) 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); e) 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 f) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or g) for the	Not Implemented

		establishment, exercise or defence of legal claims.	
3.18.1	Right to restriction of processing - Terms of restricting data processing	The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: a) 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; b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; c) 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; d) 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.	Not Implemented
3.18.2	Right to restriction of processing - Rules for processing restricted data	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.	Not Implemented
3.18.3	Right to restriction of processing - Notification obligation	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.	Not Implemented
3.19	Notification obligation regarding rectification or erasure of personal data or restriction of processing	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. The controller shall inform the data subject about those recipients if the data subject requests it.	Not Implemented
3.20.1	Right to data portability - Rights to receive personal data	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	Not Implemented

		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: a) 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 b) the processing is carried out by automated means.	
3.20.2	Right to data portability - Data transmission	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.	Not Implemented
3.21.1	Right to object - Rights	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. 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.	Not Implemented
3.21.2	Right to object - Marketing purposes	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.	Not Implemented
3.21.3	Right to object - Stop processing data after objection	Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.	Not Implemented
3.21.4	Right to object - Communication of rights	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.	Not Implemented
3.21.6	Right to object - Scientific or historical research purposes or statistical purposes	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	Not Implemented

		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.	
3.22.1	Automated individual decision-making, including profiling - Rights	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.	Not Implemented
3.22.2	Automated individual decision-making, including profiling - Paragraph 1 Exceptions	Paragraph 1 shall not apply if the decision: a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; b) 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 c) is based on the data subject's explicit consent.	Not Implemented
3.22.3	Automated individual decision-making, including profiling - Safeguarding measures	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.	Not Implemented
3.22.4	Automated individual decision-making, including profiling - Exceptions	Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(2)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.	Not Implemented
3.23.1	Restrictions - The scope of the obligations and rights	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: a) national security; b) defence; c) public security; d) the prevention, investigation, detection or	Not Implemented

		prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; e) 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; f) the protection of judicial independence and judicial proceedings; g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; h) 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); i) the protection of the data subject or the rights and freedoms of others; j) the enforcement of civil law claims.	
3.23.2	Restrictions - Specific provisions	In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to: a) the purposes of the processing or categories of processing; b) the categories of personal data; c) the scope of the restrictions introduced; d) the safeguards to prevent abuse or unlawful access or transfer; e) the specification of the controller or categories of controllers; f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; g) the risks to the rights and freedoms of data subjects; and h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.	Not Implemented
4.24.1	Responsibility of the controller - Technical and organisational measures	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. Those measures shall be reviewed and updated where necessary.	Not Implemented

4.24.2	Responsibility of the controller - Data protection policies	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.	Not Implemented
4.25.1	Data protection by design and by default - Technical and organisational measures	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.	Not Implemented
4.25.2	Data protection by design and by default - Processing only necessary data	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. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. 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.	Not Implemented
4.26.1	Joint controllers - Responsibilities	Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. 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	Not Implemented

		determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.	
4.26.2	Joint controllers - Roles and relationships	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. The essence of the arrangement shall be made available to the data subject.	Not Implemented
4.27.1	Representatives of controllers or processors not established in the Union	Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.	Not Implemented
4.27.2	Representatives of controllers - Exceptions	The obligation laid down in paragraph 1 of this Article shall not apply to: a) 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 b) a public authority or body.	Not Implemented
4.27.3	Representatives of controllers - Establishment of representative	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.	Not Implemented
4.27.4	Representatives of controllers - Mandate	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.	Not Implemented
4.28.1	Processor - Processor Engagement	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.	Not Implemented

4.28.2	Processor - The addition or replacement of other processors	The processor shall not engage another processor without prior specific or general written authorisation of the controller. 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.	Not Implemented
4.28.3	Processor - Governance	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. That contract or other legal act shall stipulate, in particular, that the processor: a) 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; b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; c) takes all measures required pursuant to Article 32; d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor; e) 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; f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing	Not Implemented

		and the information available to the processor; g) 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; h) 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.	
4.28.4	Processor - Data protection obligations in the process of engaging another processor	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. 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.	Not Implemented
4.28.6	Processor - Contractual clauses	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.	Not Implemented
4.28.9	Processor - Form of the contract	The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.	Not Implemented
4.29	Processing 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	Not Implemented

		the controller, unless required to do so by Union or Member State law.	
4.30.1	Records of processing activities - Controller - Creation and Maintenance of Processing Record	Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; b) the purposes of the processing; c) a description of the categories of data subjects and of the categories of personal data; d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; e) 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; f) where possible, the envisaged time limits for erasure of the different categories of data; g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	Not Implemented
4.30.2	Records of processing activities - Processor - Creation and Maintenance of Processing Record	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: a) 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; b) the categories of processing carried out on behalf of each controller; c) 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	Not Implemented

		documentation of suitable safeguards; d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	
4.30.3	Records of processing activities - Records' Format	The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	Not Implemented
4.30.4	Records of processing activities - Records Availability	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.	Not Implemented
4.30.5	Records of processing activities - Exceptions	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.	Not Implemented
4.31	Cooperation 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.	Not Implemented
4.32.1	Security of processing - Implementation of technical and organisational measures	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: a) the pseudonymisation and encryption of personal data; b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	Not Implemented

4.32.2	Security of processing - Risks arising from the processing	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.	Not Implemented
4.32.3	Security of processing - Elements for fulfilling the requirements	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.	Not Implemented
4.32.4	Security of processing - Application of measures to ensure that data is processed per the instructions	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.	Not Implemented
4.33.1	Notification of a personal data breach to the supervisory authority	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. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.	Not Implemented
4.33.2	Notification of a personal data breach - Data breach notice by the processor	The processor shall notify the controller without undue delay after becoming aware of a personal data breach.	Not Implemented
4.33.3	Notification of a personal data breach - The data breach notice elements	The notification referred to in paragraph 1 shall at least: a) 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; b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; c) describe the likely consequences of the personal data breach;	Not Implemented

		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.	
4.33.4	Notification of a personal data breach - Provision of information related to the breach	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.	Not Implemented
4.33.5	Notification of a personal data breach - Documenting data breach	The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.	Not Implemented
4.34.1	Communication of a personal data breach to the data subject	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.	Not Implemented
4.34.2	Communication of a personal data breach - Format of the data breach notice	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).	Not Implemented
4.34.3	Communication of a personal data breach - Exceptions	The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: a) 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; b) 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; c) 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.	Not Implemented

4.34.4	Communication of a personal data breach - The supervisory authority	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.	Not Implemented
4.35.1	Data protection impact assessment - Carrying out the impact assessment	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. A single assessment may address a set of similar processing operations that present similar high risks.	Not Implemented
4.35.2	Data protection impact assessment - Advice of the data protection officer	The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.	Not Implemented
4.35.3	Data protection impact assessment - Cases requiring impact assessment	A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: a) 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; b) 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 c) a systematic monitoring of a publicly accessible area on a large scale.	Not Implemented
4.35.4	Data protection impact assessment - List of operations requiring impact assessment	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. The supervisory authority shall communicate those lists to the Board referred to in Article 68.	Not Implemented
4.35.5	Data protection impact assessment -	The supervisory authority may also establish and make public a list of the kind of processing	Not Implemented

	List of operations not requiring impact assessment	operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.	
4.35.7	Data protection impact assessment - Elements of assessment	The assessment shall contain at least: a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and d) 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.	Not Implemented
4.35.9	Data protection impact assessment - Seek the opinion of data subjects	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.	Not Implemented
4.35.10	Data protection impact assessment - Exceptions	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.	Not Implemented
4.35.11	Data protection impact assessment - Reviewing to assess if the processing is performed	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.	Not Implemented
4.36.1	Prior consultation - Consultation with the supervisory authority	The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article	Not Implemented

		35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.	
4.36.3	Prior consultation - Elements of the request for consultations	When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with: a) 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; b) the purposes and means of the intended processing; c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation; d) where applicable, the contact details of the data protection officer; e) the data protection impact assessment provided for in Article 35; and f) any other information requested by the supervisory authority.	Not Implemented
4.37.1	Designation of the data protection officer - Terms of appointment	The controller and the processor shall designate a data protection officer in any case where: a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; b) 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 c) 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.	Not Implemented
4.37.2	Designation of the data protection officer - Appointing a single data protection officer	A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.	Not Implemented
4.37.3	Designation of the data protection officer - Data protection officer for public	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.	Not Implemented
4.37.5	Designation of the data protection officer - Competences	The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection	Not Implemented

		law and practices and the ability to fulfil the tasks referred to in Article 39.	
4.37.6	Designation of the data protection officer - Appointing a staff member	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.	Not Implemented
4.37.7	Designation of the data protection officer - Publishing the officer's contact details	The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.	Not Implemented
4.38.1	Position of the data protection officer - Ensuring the data protection officer's involvement	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.	Not Implemented
4.38.2	Position of the data protection officer - Supporting the data protection officer in performing tasks	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.	Not Implemented
4.38.3	Position of the data protection officer - Responsibilities of the data protection officer	The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.	Not Implemented
4.38.4	Position of the data protection officer - Contacting data protection officer regarding any processing issues or questions	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.	Not Implemented
4.38.5	Position of the data protection officer - Ensuring the secrecy and confidentiality	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.	Not Implemented
4.38.6	Position of the data protection officer - Avoiding conflict of interest	The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.	Not Implemented

4.39.1	Tasks of the data protection officer - Tasks	The data protection officer shall have at least the following tasks: a) 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; b) 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; c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; to cooperate with the supervisory authority; d) 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.	Not Implemented
4.39.2	Tasks of the data protection officer - Data processing risks	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.	Not Implemented
5.44	General principle for transfers	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. 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.	Not Implemented
5.45.1	Transfers on the basis of an adequacy decision -	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	Not Implemented

	International Organization transfer	specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.	
5.46.1	Transfers subject to appropriate safeguards - Conditions	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.	Not Implemented
5.46.2	Transfers subject to appropriate safeguards - Provision	The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: a) a legally binding and enforceable instrument between public authorities or bodies; b) binding corporate rules in accordance with Article 47; c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2); d) 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); e) 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 f) 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.	Not Implemented
5.46.3	Transfers subject to appropriate safeguards - Conditions for proper protection measures	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: a) 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 b) provisions to be inserted into administrative arrangements between public authorities or bodies which	Not Implemented

		include enforceable and effective data subject rights.	
5.47.1	Binding corporate rules - Consistency mechanism	The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they: a) 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; b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and c) fulfil the requirements laid down in paragraph 2.	Not Implemented
5.47.2	Binding corporate rules - Guidelines and Specifications	The binding corporate rules referred to in paragraph 1 shall specify at least: a) 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; b) 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; c) their legally binding nature, both internally and externally; d) 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; e) 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; f) the acceptance by the controller or processor established on the	Not Implemented

		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; g) 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; h) 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; i) the complaint procedures; j) 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; k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority; l) 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); m) 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 n) the appropriate data protection training to personnel having permanent or regular access to personal data.	
5.49.1	Derogations for specific situations	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: a) 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; b) 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; c) 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; d) the transfer is necessary for important reasons of public interest; e) the transfer is necessary for the establishment, exercise or defence of legal claims; f) 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; g) 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	Not Implemented

		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.	
5.49.6	Derogations for specific situations - Document assessment	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.	Not Implemented