# Catalogue of security measures

Here you will find a catalogue of technical and organizational security measures developed by the Danish Data Protection Authority that companies and authorities can consider in various contexts when implementing privacy programmes.

## Table of Contents





White Label Consultancy

## About the catalogue

The catalogue is a collection of descriptions of technical and organizational measures that may be relevant to consider in order to ensure adequate security, cf. the General Data Protection Regulation (GDPR) Article 5 and Article 32. The assessment of whether the individual measures and described measures are necessary is made by the organization based on a concrete risk assessment. The value of measures can depend a lot on which other measures have been established, and the catalogue is therefore neither exhaustive nor absolute in relation to whether the necessary steps have been taken to achieve a sufficient degree of processing security.

The descriptions of the individual measures can be read individually, so that the catalogue can function as a reference work.

Many measures can be implemented as part of the functions that support data protection in IT systems in general and are thus also relevant in relation to the obligations under the Article 25 GDPR on the duty to ensure that data protection is considered in the design and default settings when developing or acquiring new IT systems or development/change in existing IT systems.

The examples used are largely based on the Danish Data Protection Authority's experience from supervision of private and public companies, treatment of breaches of personal data security notified to the Data Protection Authority, the EDPB's guidelines and the ISO standards 27001 (Danish Standard DS/ISO/IEC 27001 – Requirements for Information Technology – security techniques – Information Security Management Systems (ISMS)) and 27002.

## What is a measure?

Measures are measures that preserve and/or change a risk. A measure can be preventive, detection, corrective or a combination of these. This is explained in more detail in the description of each measure.

Technical measures with relevance for rights management are, for example, IT solutions for user administration, automatic encryption/deletion, automatic access control (log-in), registration of uses of personal data (logging), physical doors and locks.

Organizational measures with relevance for rights management are, for example, security policies, procedures for regular control of access rights, procedures for withdrawing access rights in the event of dismissal and resignation, distribution of tasks according to competences, training in the correct use of IT solutions (i.e., competences), assessment and evaluation of the effectiveness of technical and organizational measures.

In standards and textbooks, measures may be divided into further categories, e.g., "physical", "person-related" or "behavioural". However, the GDPR only describes the categories "technical"

and "organizational", so the examples above cover it all. When it says, for example, "physical locks", this can be described as a physical measure, but also as another technical measure. Training can be described as a person-related or behavioural measure, but also as yet another organizational measure.

It is not decisive in which category a measure can be placed. What is crucial is that sufficient measures have been established to ensure a level of security that can protect the processing of personal data - and the business.

For a firewall to have a protective effect, more is needed than purchasing and installing a software or hardware firewall. A firewall must be set up, managed and kept up-to-date properly, and an organization will typically benefit from multiple firewalls that are managed differently. A measure that is described as a "Firewall" will therefore actually consist of many measures - often a mixture of something technical and something organizational. These measures could each be described as independent measures, but to avoid confusion they are called "measures" in this catalogue.

## Measure:

### Access rights as needed

#### WHAT RISKS ARE ADDRESSED?

If an employee has access to an IT system that is wider than the work-related need, it can pose an unnecessary risk of loss of data *confidentiality* and *integrity* through the employee's mishandling or actual misuse. Too broad access to add, change or delete data poses an unnecessary risk of loss of data *integrity* and *availability*. Limiting access rights (e.g. read access without write access) can prevent errors and misuse. It is therefore a *preventive* measure which can reduce *the consequences* if a user access is used incorrectly or abused.

The same is not usually the case with a citizen's/customer's access to a self-service solution, as the options (read, change, add, delete data) are usually chosen based on what the user of the self-service solution must be able to do themselves, and the responsibility for incorrect use/misuse lies with the user himself. However, there may be exceptions to this, where it is inappropriate to give the customer the opportunity to change/delete certain data, even if it is the customer's own personal data.

#### WHAT MEASURES CAN BE CONSIDERED?

Access rights for employees are adapted to a work-related need and are limited in, for example, opportunities to read, add, search, change, extract or delete data.

If RPA (Robotic Process Automation) or similar is used, and access rights are given to robot users in this connection, their access is similarly restricted as much as possible. Financial savings on robot user licenses can be tempting to give a robot as many access rights as possible, but a robot user who has many rights can pose a higher risk if, for example, a hacker gets the opportunity to obtain this robot's access rights. By minimizing the access rights of robot users, the potential damage that the robot user can do in the event of an error in the code/automation is also limited.

The options for restricting access rights usually depend on the design of the IT systems, which is why these aspects are taken into account at the time of design, purchase of or changes to existing IT systems.

Certain access rights can give the opportunity to do irreparable damage, e.g. deletion, and are therefore granted to as few people as possible and only to people with the right skills. This measure must therefore be seen in the context of the measure Correlation between user competences, access rights and tasks.

## WHEN IS THE MEASURE NECESSARY?

Article 5(1)(f) GDPR is about the integrity and confidentiality of personal data. The less the individual user can do with the data to which the user has access, the less the potential consequence if some of these users take unintended or malicious actions or unwarranted uses of data. This also has a protective effect in relation to cyber threats, as a hacker often operates through access rights in compromised user accounts, and fewer rights thus limit the hacker's options. Access rights must therefore be limited as much as possible.

Article 25 GDPR: When developing or acquiring a new IT system or developing/changing an existing IT system, data protection must be considered in the design and default settings. The option to limit/differentiate access rights to data requires that the option is built into the IT systems that control access.

# Measure:

## Awareness

### WHAT RISKS ARE ADDRESSED?

Awareness is used as a collective term for all the attention-oriented initiatives that can increase employees' awareness and knowledge of safety aspects. It can be about what employees are not allowed to do, or what they *should/must* do. It is therefore typically about motivating employees to a less risky or changed behavior when handling data. It is therefore a *preventive* measure that can reduce *the likelihood* of many different scenarios that can affect the confidentiality, integrity or availability of data.

It can be measures that train employees to spot phishing messages, where a fraudster tries to steal the employee's login information via e-mail or SMS. If employees fail to provide such information, click on suspicious links or open attachments, one may avoid compromising user access or the organization's network. Awareness can also be information to employees that all actions in IT systems are logged in the hope of preventing abuse.

If employees learn what to do to quickly block a lost/stolen access card, awareness can also provide a detection measure, potentially stopping an incident (lost/stolen access card) before the incident impacts the organisation's processing of personal data (the card is misused to access data/papers).

### WHAT MEASURES CAN BE CONSIDERED?

The following is a list of measures from which to choose, depending on what is relevant in the individual organization and in relation to the individual processing of personal data.

Several of the measures can also be supported technically, so that users cannot avoid doing the right thing. Initiatives which are solely based on procedures that must be remembered and complied with inherently involve a risk of non-compliance. This risk can often be minimized to a significant extent through technical support.

- Ensuring knowledge of which actions are logged, the purpose of the logging and possible sanctions for abuse of, for example, access rights. This may include logging of the user's actions in IT systems, but also logging of physical access to premises, TV surveillance, etc.
- Authorization officers, user administrators and users are informed about what they are allowed to do with their respective access rights, e.g.:
    - that users may not use data for other than work-related purposes,

    - that authorization officers must focus on limited access (not only on the users' ability to solve tasks), and
    - that user administrators must not act on their own and must document all authorizations issued by the authorization officers.
- Guidance on choosing passwords, including avoiding codes that are also used privately, as these may be compromised or not sufficiently secure.
- Strengthening information that passwords, tokens, access cards and other access-granting factors are strictly confidential and personal, and that the user is responsible for all actions performed during their login – possibly with reference to logging and penalties. This can be supported with information on fixed procedures for sampling and auditing.
- Instructions on how users should react in the event of suspicion/knowledge that an unauthorized person has gained access/knowledge of access-granting factors.
- Instructions on how users must react in the event of suspicion/knowledge that unauthorized persons have gained access to access media such as keys, key fobs, access cards, etc. Even if there is only electronic access to personal data, this instruction may be relevant if:
    - the access medium provides physical access to IT equipment that contains personal data, or
    - the level of security in the electronic access is different, depending on where you are physically – for example inside or outside the organisation's office building.
- Specific knowledge of how personal data may be used for testing in connection with the development of IT systems.
- Orientation on the consequences of breaking rules/legislation on confidentiality and any signed non-disclosure agreement.
- General knowledge of how personal data can and must be processed in accordance with the GDPR and other relevant legislation, for example by following internal guidelines which have been made to ensure implementation of legislation. This may concern storage, use, disclosure, deletion, transmission and other processing. Special attention to the fact that some "ordinary" personal data may be confidential, e.g. protected addresses.
- Targeted guidance in the use of specific IT systems, e.g. journaling, publication, journaling with automated publication, anonymization, removal of hidden metadata (data about data, e.g. information about a file as opposed to the file's content), requirements from legislation, etc. combined with tools that make it easier to perform the aforementioned actions without making mistakes.
- Targeted guidance for user administrators or IT security officers in spotting internal abuse attempts.
- Targeted guidance for employees with access to the organization's bank accounts and financial systems regarding "CEO fraud" (also known as "director fraud"), where employees are cheated by someone pretending to be a director. This may

possibly combine with other business rules that support proper approval of pay-outs and currency transfers.

Here you can read the Center for Cyber Security's description of a method for working with behavior related to information security.

## WHEN IS THE MEASURE NECESSARY?

Since awareness can reduce many very different risks, it cannot be specified when the measure is necessary. Awareness is an organizational (including person-related/behavioural) measure. It usually constitutes a supplement to handling threats that cannot be adequately handled via technical (including physical) measures. Therefore, the need for awareness depends on how much can be secured in other ways.

## Measure:

### Automatic closing of inactive accesses

#### WHAT RISKS ARE ADDRESSED?

More user accesses provide a larger "attack surface" for malicious actors – they have, so to speak, more bricks to build their attacks with. Inactive accesses therefore pose an unnecessary risk. This is therefore a *preventive* measure which can reduce the *likelihood* that an (unnecessary) user access is misused.

Inactivity is often a sign that the access is unnecessary, and inactive accesses can more easily be misused for a longer period of time without the rightful user discovering it, because he does not use the access himself.

#### WHAT MEASURES CAN BE CONSIDERED?

Automatic closure of accesses that have not been used for a period of time - for example 40 days - is established. Where the function is built into the IT system, it is selected. Alternatively, a manual procedure is established. To ensure uniform administration, it is managed centrally from a user management system as far as possible, instead of locally in the individual subject systems.

#### WHEN IS THE MEASURE NECESSARY?

The above measures do not eliminate the need for other measures concerning the closing of unnecessary access. Unnecessary access must be closed as soon as possible to minimize the aforementioned "attack surface". Furthermore, a user may choose to deliberately use an access at regular intervals to bypass the automatic closing.

It is a risk assessment according to Article 32 GDPR that will show which measures are relevant. The measures do not in themselves ensure against *deliberate* abuse, and the value of the measures depends a lot on what else is done to ensure the rapid closure of unnecessary access.

Article 25 GDPR: When developing or acquiring a new IT system or developing/changing an existing IT system, data protection must be considered in the design and default settings. Automatic closing requires that the functionality is built into the IT system that controls access.

# Measure:

## Backup

### WHAT RISKS ARE ADDRESSED?

Backup can be used to re-establish access to data that has become inaccessible or destroyed by, for example, malicious software or an IT crash. This is therefore a *corrective* measure which can reduce the consequences of accidental or illegal destruction, loss or alteration of data.

You could say that a backup makes "loss of availability" a *temporary* loss rather than a *permanent* loss. Backup can also be used to correct the integrity of the data, if the data is, for example, compromised by a computer virus or hacker.

Backup can be about other than data in the form of e.g., personal data. This may involve securing the possibility of being able to restore entire systems and thus backup e.g., operating systems, databases, certificates, encryption keys, licenses, system settings (including firewall settings), which are complex and time-consuming to restore manually.

The effect of backup is very dependent on the time factor – how long does it take from the loss of availability/integrity and when the backup is used until data can be restored? If, for example, only a very short time has to pass with data being unavailable before the consequence is at maximum, it may be that backup cannot solve this (alone), and that duplicate IT systems must be used.

Backup cannot restore an IT system as it was exactly when an incident occurred, rather as it appeared some time *before* the incident. Thus, backup is also characterized by the fact that there is usually always a risk of data loss which cannot be eliminated – yet this risk is smaller when using duplicate data/systems.

As backups usually do not include the last changes to data, there will still be a (minor) problem with data integrity after a backup is used to restore data. Likewise, the backup may include data that has been deleted from the IT system and which must therefore be deleted again after the backup has been used.

Backup should not be confused with a "copy of data". Backup is much more than a copy of data and can therefore also protect against several threats. Some threats (e.g., ransomware) are designed to affect both data on the IT system and the copy of the same data, and therefore a copy of data is often only a false sense of security.

## WHAT MEASURES CAN BE CONSIDERED?

Backup of data: Copies of data are constantly being backed up. Data is stored in a way that cannot be deleted – also called WORM (Write Once, Read Many).

Procedures for assigning access ensure that the same person does not have access to both production data and the copy of this data. Where this cannot be avoided, the accesses are shared, requiring different user accounts to access them.

Intervals between backups: The longer the time that elapses between data being copied to backups, the greater data loss can be experienced if backups must be used to re-establish access to data. The time that elapses between each copying of data is determined on the basis of the risk assessment – i.e., an assessment of how long ago the last copy must have been taken before the consequences could be too great for the data subjects. In a backup strategy, intervals and the type (full/incremental copies) are specified.

Alarm: If the backup is automated, an alarm ensures that it is detected if the automatic backup fails.

Backup of software and hardware: It examines which hardware and software can be recovered and how quickly. This applies, for example, to physical servers, operating systems, database software, licenses, encryption keys, etc. Alternatively, it ensures that these elements are also found in a copy.

Physical location of the backup copy: The physical location is determined based on the risk assessment, i.e., based on an assessment of which threats may affect the physical location where the original data is located. If, for example, there is a possibility that IT systems are destroyed by a flood, then the copy is placed in a place that cannot be affected by the floods caused by a storm.

Logical location (network location): Backup is stored in a place where there is more limited access, as only a few (IT administrators) need the access. The networks that store production data and backup data are not network-connected, e.g., because the backup is with a backup supplier. Where this cannot be avoided, the networks are segmented from each other via firewalls, which limit access to what is absolutely necessary, so backup is better protected against hacker attacks that can affect other parts of the network.

Backup copy testing: It is tested at regular intervals whether the backup is carried out at the expected intervals (frequency), whether the backup copy is available, whether the backup copy contains all relevant data (extent), whether the backup copy is truthful (integrity). The latter can, for example, be a type of integrity test (checksum or other).

Restoration testing: It is tested whether data can actually be reloaded and used in an IT system. This is a test of (1) whether recovery can be done with existing guides/procedures, (2) that everything that has copies (hardware, software, data) can work together, and (3) that

recovery can happen quickly enough in relation to the fact that the consequence usually increases with time (Recovery Time Objective).

Deletion after backup: Procedures are laid down to ensure that data that must be deleted is deleted again after using a backup, so that data is not stored for longer than necessary, cf. herewith Article 5 GDPR.

It is ensured that the use of backup – and thus the spread of data – does not increase the risk to the data subjects. This is done by the fact that the transmission and storage of data in backup is secured against unauthorized access, and that the handling of data in backup takes place under the control of the data controller. This is done through data processing agreements and by encrypting data before transfer and storage.

## WHEN IS THE MEASURE NECESSARY?

It is primarily a risk assessment according to Article 32 GDPR that will show which measures are relevant, as risks are very dependent on the consequence for the rights of the data subjects – rights that are affected if their personal data ceases to be available to the data controller.

If, for example, we are talking about patient records in a hospital, then lack of availability can have an impact on whether the patient can receive the optimal treatment - in the worst case, it can have fatal consequences. If, on the other hand, it is a customer register for an online store that sells dresses, there is presumably less or no consequence for those registered in the event of lack of availability.

## Measure:

### Centralized Rights Management

#### WHAT RISKS ARE ADDRESSED?

Decentralized (or "autonomous") rights management can mean that whoever performs rights management does not have it as their main task. It can increase the possibility of errors due to lack of experience, knowledge or lack of focus on security when managing access rights.

If changes occur in an IT environment without rights management being continued and tested, it can, among other things, cause the relevant access restriction to disappear, so that unauthorized access immediately occurs. Decentralized rights management may imply a greater likelihood that specific conditions of importance for rights management will be overlooked when changes are made to IT environments, because only one or a few people are aware of the conditions in question.

If rights management is instead carried out by a central unit that has it as its main task, it is easier to ensure the necessary knowledge and focus on security. This prevents errors. This is therefore a preventive measure which can reduce the likelihood of unnecessary user access being established or maintained.

Centralized rights management will usually also make it easier to control, and thus to implement the measure Periodic control of the timeliness of access rights.

#### WHAT MEASURES CAN BE CONSIDERED?

An overview of all user accesses and uniform management of these is ensured. The task is gathered organizationally with people who receive the necessary training to handle this particular task.

Via guidelines and/or technical measures, decentralized user administration is prohibited/prevented. For example, by deciding that only employees in the central user administration unit can manage access rights. A technical measure can, for example, be a technical obstacle to employees being able to create folders with access restrictions on network drives or web-based file sharing platforms such as SharePoint.

The centralization can include a technical centralization via the use of Single Sign-On or a Directory Service such as Active Directory in Windows. If possible, there should be a link to authoritative systems, for example an HR system that always shows who is currently employed

and in which position/department. If possible, there should be a link to a centralized rights allocation via, for example, an IdM system.

Where centralized rights management is not possible or appropriate, fixed procedures for execution are established instead, so that uniform principles are followed, similar to what happens in centralized rights management. Attention is also ensured to decentralized rights management in the event of future changes in that part of the IT environment, which is why it is also part of the Change Management measure.

## WHEN IS THE MEASURE NECESSARY?

It is primarily a risk assessment according to Article 32 GDPR, which must show which measures are relevant, as risks and opportunities are very dependent on the specific organization and on which types of IT systems are used.

Article 25 GDPR: When developing or acquiring new IT systems or developing/changing existing IT systems, data protection must be considered in the design and default settings. If IT systems are selected/designed to be part of a central rights management and possibly Single Sign-On, a decentralized rights management with the aforementioned risks can be avoided.

## Measure:

### Data access as needed

#### WHAT RISKS ARE ADDRESSED?

Access rights must be limited as much as possible. When an employee has access to many people's information, it can increase the temptation to abuse the access for private or non-work-related purposes. By limiting data access so that it corresponds to work-related needs, the possibilities for abuse can be reduced. This is therefore a *preventive* measure which can reduce *the likelihood* of misuse of user access, and *the consequences* if misuse were to take place.

The same is usually also the case with a citizen's/customer's access to a self-service solution at an authority or a private company, as access must often be limited to the user's own personal data.

#### WHAT MEASURES CAN BE CONSIDERED?

Access for employees is granted according to work-related needs and can be limited to, for example, the timeliness or age of the data, data type (e.g. whether it is customer data, HR data, whistle-blower data), case type (e.g. "Road & park" or "family cases"), etc.

Access rights for citizens/customers are adapted to what the individual has the right to access (typically only their own and possibly close relatives' personal data).

The options usually depend on the design of the IT systems, which is why these aspects are taken into account at the time of designing or purchasing IT systems.

If RPA (Robotic Process Automation) or similar is used, and access rights are given to robot users in this connection, their access is similarly restricted as much as possible. Financial savings on robot user licenses can be tempting to give a robot as many access rights as possible, but a robot user who has many rights can pose a higher risk if, for example, a hacker gets the opportunity to obtain this robot's access rights. Robot users' access rights are also minimized due to possible errors in the code/automation or setup. This limits the potential damage that the robot user can cause.

See also the measure Pseudonymisation and anonymisation, which also restricts access, but by removing or separating data.

## WHEN IS THE MEASURE NECESSARY?

Article 5(1)(f) GDPR is about the integrity and confidentiality of personal data. The less data the individual user has access to, the less the potential consequence if some of these users take unintentional or malicious actions or otherwise abuse access to data. At the same time, this also has a protective effect in relation to cyber threats, as a hacker often operates through access rights in compromised user accounts, and fewer rights thus give the hacker fewer opportunities. Access rights must therefore be limited as much as possible.

Article 25 GDPR: When developing or acquiring new IT systems or developing/changing existing IT systems, data protection must be considered in the design and default settings. The option to minimize access rights requires that the option is built into the IT systems that control access. Default settings can also minimize rights as a starting point, but it can also be about, for example, automatic deletion of data according to their age, which contributes to minimizing data access.

## Measure:

### Documentation of authorizations

#### WHAT RISKS ARE ADDRESSED?

User administrators have the option of giving others – and usually themselves – access to IT systems. The user administrator has the technical possibility to create access without following established procedures or authorisations, for example to facilitate proceedings or in the worst case to create a basis for abuse. Requirements for documentation for the necessary authorization are a counterweight to this. This is therefore a preventive measure that can reduce *the likelihood* that a user administrator makes mistakes or abuses his access rights.

#### WHAT MEASURES CAN BE CONSIDERED?

Procedures and/or technology are set up in such a way that user administrators are forced to document that they have not acted on their own in relation to issuing access rights to others or oneself.

There is a (written) requirement that authorizations (authorization officers' approvals of access rights) be documented by the user administrator. This protects against a user administrator being pressured to issue access rights without documented authorization – this kind of pressure could, for example, come from a manager who is more focused on streamlining workflows than on security. The user administrator keeps the documentation to be able to show that correct procedures have been followed when assigning access rights.

As far as possible, a technical obstacle is created so that the user administrator can change the authorization once it has been submitted and documented. This protects against cheating on the part of the user administrator.

It is supplemented with ad hoc checks of whether the documentation matches established access rights. It may possibly happen as part of the measure Periodic control of the timeliness of access rights .

#### WHEN IS THE MEASURE NECESSARY?

Article 5(1)(f) GDPR states, among other things, that personal data must be processed in a way that ensures protection against unauthorized or illegal processing. When authorizations are not documented, it can reduce the sense of responsibility of both the user administrator and the

authorization officer. Thus, making daily life work can be given higher priority than performing rights management correctly.

It is primarily a risk assessment according to Article 32 GDPR, which must show which measures are relevant, but considering the human aspect, documentation of authorizations will very often be relevant.

## Measure:

### Multi-Factor Authentication (MFA)

#### WHAT RISKS ARE ADDRESSED?

Multi-factor authentication is also called multi-factor login or in English MFA (Multi-Factor Authentication).

The purpose of this measure is to strengthen control over who accesses an IT system, so that the likelihood of unauthorized access is minimized.

"Authentication" is about a person verifying his identity. The user of an IT system can, for example, verify his identity by providing a password that only the user should know. The password is thus the authenticating factor in the login process.

MFA requires the user to submit two or more independent factors of different categories to gain access. Two factors are considered independent if it is not possible to derive one factor from knowledge of the other factor. The various categories are described below (A, B, C), and the risk picture is affected by which categories are selected for the login process.

It may also be considered as a detection measure: Attempts to gain unauthorized access through an authorized user's login will require multiple steps (due to the multiple factors in the login process) and may provide an increased opportunity to detect abuse attempts in progress (on the first factor) and before it ends in a successful unauthorized access.

#### WHAT MEASURES CAN BE CONSIDERED?

The factors must be able to authenticate who the user is, i.e., ensure that it is the right user who logs in.

Username, customer number, social security number (CPR number), etc. cannot be considered a factor if anyone other than the user knows or has access to this information. Furthermore, it is information of the same nature and is entered in the same way as the password, which is why they are exposed to the same threats (e.g., eavesdropping via malware or physical surveillance). Therefore, having to enter both username and password does not significantly reduce risks - even if both were known only to the user themselves. The factors are selected from different categories of the following:

- Something the user knows: Typically, a personalised password. It must be something that only the user knows, and that the user can only memorise. Therefore, it is usually also

something that the user has chosen themselves. The factor must not at any time have been accessible or become accessible to other people, which is why it must be stored one-way encrypted (hashed). The user must be able to replace this factor if it is suspected that others have gained knowledge of it.

- Something the user has: For example, a personalised card with unique one-time codes. The factor can also be generated by unique software embedded in hardware, e.g. one-time codes from a hard key/key fob. It must be something that the user can have in their physical possession and that they can keep completely to themselves. It must not be something that needs to be shared with others. The user must be able to replace this factor if it is suspected that others have the ability to use a copy of the hardware/software.
- Something the user is: Typical biometrics, such as fingerprint, iris scan, facial recognition, voice recognition, etc. In comparison to categories A and B, category C has a built-in weakness, namely that the user can rarely keep the factor to themselves or replace it. The strength of multi-factor authentication is that it can minimise specific risks. First, all the threats that a specific login can be exposed to are identified, and then the factors are selected based on an assessment of whether they sufficiently affect (reduce) the specific risks. Example: 1. an employee must use passwords entered via PC/smartphone. This can be done by the employee in public places. A primary threat is that the password can be intercepted by malicious software or hackers who have compromised the PC/smartphone used. The password is also subject to interception by "looking over the shoulder" or via surveillance cameras in a public place.

If the second factor is a one-time code from an electronic code viewer, this can also be intercepted in the same way and is therefore subject to the same threats as the password. However, if the code shown on the code viewer can only be used once and within a very short period of time - and the user is likely to use it immediately - then this factor is not exposed to the same degree.

The code viewer can be stolen (threat of physical theft), but the password is not exposed in the same way if it is known only to the user. Therefore, the user must not write the code on a scrap of paper that can be stolen along with the code viewer. Therefore, an organisational measure is added in the form of guidelines for users on how to handle the password and quickly report theft in order to block the code viewer and possibly the login. It can also be considered as two factors if a physical barrier must first be forced into a locked building with a personalised electronic key card ("something you have"), combined with a login to the IT system with a password ("something you know"). In this example, however, it's a little difficult to assess risks because the two factors are very separate and may be managed very differently.

The single factor is protected against misuse, making it more difficult to circumvent. For example, login functions that use the "password" factor are protected against brute force attacks and dictionary attacks that attempt to guess/test the factor. Additional protection can be established via organisational measures in the form of instructions to employees, e.g., requirements for choosing and handling passwords.

Protection against attacks where the user is tricked into handing over the access-granting factors is called Phishing-Resistant MFA. Read more about this here.

Factors are further protected by refraining from transmitting factors via e-mail and SMS, because here they are exposed to being intercepted. Factors can instead be generated locally on a device.

Finally, it is ensured that there are no detours to login, which actually undermine the multi-factor authentication solution. It could, for example, be a help solution for users who have forgotten their password, which in practice allows for login with only one factor.

See also the Center for Cyber Security's guidance on password security, which also mentions multi-factor authentication.

## WHEN IS THE MEASURE NECESSARY?

It is primarily a risk assessment according to Article 32 GDPR that will show which measures are relevant, as risks and opportunities are very dependent on the specific circumstances.

Note, however, Article 5(1)(f) GDPR, which states that personal data must be processed in a way that ensures protection against unauthorized or illegal processing. When accessing particularly sensitive personal data via the Internet, it may be impossible to adequately protect this through a login with only one factor. For access via the internet to IT systems where personal data of a nature worthy of protection is processed, multi-factor authentication or something that correspondingly increases the level of security must be implemented.

Also, in the case of login functions that are not accessible from the Internet, multi-factor authentication may be deemed necessary, e.g., because it is an administrator's access, which must be particularly well protected against threats that are located on (or can move into) the organization's internal networks.

# Measure:

## Separation of functions

### WHAT RISKS ARE ADDRESSED?

Tasks performed with one access right may disqualify the person from tasks that can be performed with another access right. This is why separation of functions is known from financial systems, where it ensures that one employee alone can correct and approve an invoice for own purchases.

In the same way, the same person must not be able to order and authorize their own access to an IT system. This is avoided by establishing functional separation in tasks and/or access rights. It is therefore a preventive measure which can reduce the likelihood of various types of abuse of access rights.

Separation of functions is there with a measure that supports mutual control between different work functions and thus prevents abuse.

### WHAT MEASURES CAN BE CONSIDERED?

Procedures are established - if technically possible - by which functional separation is ensured between users (those who use access), those responsible for authorization (those who approve access) and user administrators (those who create/remove access). There can also be a fourth link, if, for example, an IT operations employee in practice creates/removes access on behalf of the user administrator.

Separation of functions is carried out by a sharp separation of work tasks and access rights, where the tasks/accesses of the above-mentioned persons do not overlap as far as possible. For example, a user administrator must not approve his own access to an IT system, and if this cannot be prevented technically, there must be an approval procedure which ensures valid documentation for the authorization officer's approval. With manual form-based procedures, it may be necessary to design the authorization form so that it cannot be corrected after the authorization officer has approved access.

Rules are set against, or a technical obstacle is established for an authorization officer to approve changes to his own access.

If the option is present in the IT system, the user administrator's access rights are limited to only allow rights management in the IT system. Thus, the user administrator cannot himself access data in the IT system where he/she controls others' access to data.

When assigning new access in relation to new employment or reassignment in the organization, procedures or descriptions are laid down which ensure that a situation cannot arise where an employee gains access across the desired separation of functions. It may possibly is secured through the form used when granting access rights.

It is ensured that access, which only has an IT operational purpose, is only given to IT operations personnel with the right training, and if possible, also for a limited time.

Separation of functions is not only relevant between humans, but also between robots. If RPA (Robotic Process Automation) or the like is used, and access rights are given to robot users in that connection, it may appear as if the lack of separation of functions does not entail the same risks as if the same rights were combined with one natural person. Financial savings on robot user licenses can be tempting to give a robot as many access rights as possible, but this can pose a higher risk if, for example, a hacker or software developer gets the opportunity to abuse this robot's rights.

## WHEN IS THE MEASURE NECESSARY?

Article 5(1)(f) GDPR is about the integrity and confidentiality of personal data, and this is usually not secured well enough, without a certain degree of functional separation. However, the data controller's risk assessment according to Article 32 GDPR may indicate that functional separation is not necessary in relation to specific processing of personal data.

The possibility of implementing this measure can also be limited by the size of the organisation, and therefore functional separation cannot be expected in, for example, a two-person company.

## Measure:

### Management of temporary user accounts

### WHAT RISKS ARE ADDRESSED?

More access provides a larger "attack surface" for malicious actors – they have, so to speak, more bricks to build their attacks with. Accesses that are no longer necessary therefore pose an unnecessary risk and must therefore be closed. Advance knowledge of when an access is no longer needed can be used to ensure quick closure of the access. It is therefore a preventive measure that can reduce the likelihood that an access will be misused by someone other than the intended (authorized) user.

### WHAT MEASURES CAN BE CONSIDERED?

If the option exists, an expiry date will already be set on the right of access when access is established. It may possibly be managed centrally via data from an HR system with updated information on resignation dates. Expiration date can be relevant, for example, when hiring external consultants linked to a project with a clear time horizon. Alternatively, it can be done manually with reminders in a calendar function.

Expiration date measures can also help with the backlog of tasks regarding employment and resignation, which can happen at the turn of the month or simply a random accumulation of tasks, which means that there is no time to close all access exactly when an employment stops.

In larger organisations, the measure Centralized rights management may prevent the accumulation of tasks and support a more systematic solution to the task.

### WHEN IS THE MEASURE NECESSARY?

It is a risk assessment according to Article 32 GDPR that will show which measures are relevant. If, for example, the organization has few employees, or if hiring or resignations are rare, written procedures may be sufficient, and this measure will not contribute significantly to safety.

Article 25 GDPR: When developing or acquiring new IT systems or developing/changing existing IT systems, data protection must be considered in the design and default settings. Automatic closing of access requires that the functionality is built into the IT systems that control access.

## Measure:

### Avoid unnecessary use of multi-user accounts

#### WHAT RISKS ARE ADDRESSED?

Multi-user accounts are characterized by access that can be used by several users, and therefore correspond in reality to an impersonal or anonymous login to IT systems. Actions performed during such a login cannot therefore be attributed to a single natural person, which limits the possibility of checking whether a specific use or access to information has been justified. It can be about, for example, test user accounts, which are used by different developers in turn, without it being clear who has logged in and when. In the health sector, it may be about access to equipment in examination rooms (Health Centres), where several specialist groups are with a patient at the same time.

Multi-user accounts can be a temptation for abuse. Furthermore, logging measures will have little or no preventive effect against abuse if users know they can hide behind such an anonymous login.

Avoiding or limiting the use of multi-user accounts is thus a preventive measure that can reduce the likelihood of access rights abuse. The benefit is not limited to deliberate misuse. When several people share a login, they effectively share responsibility for the processing of personal data that takes place via this login, and when several people share responsibility, the individual often feels less or no responsibility. This is a psychological effect. Finally, anonymous access can increase the likelihood that the access factors (e.g., password) are not handled properly - for several reasons:

- Passwords can be shared between people who have not necessarily been authorized. The individual user does not feel a great responsibility to protect the password, because it is already shared with colleagues.
- The passwords may not be changed when people leave the user group and thus should no longer have access.
- Passwords that the user has not chosen themselves are often more difficult to remember and are therefore written down.

#### WHAT MEASURES CAN BE CONSIDERED?

IT systems and procedures are set up in such a way that anonymous access is prevented as far as possible. This means that access factors (e.g., passwords) are personal and only known to the individual user.

Any service accounts whose login is encoded in software are protected against misuse.

If user IDs are reused (passed on to another person), it is recorded when this has happened. In this way, the organization always knows who has been able to use this user ID at any given time. This is typically the case with user accounts used for testing or temporary employment (external consultants, temps, students).

If it is not possible to avoid the sharing of access-granting factors between several people, procedures are laid down that can ensure that a change in the user group also results in a change in the access-granting factor. This means that only the current user group can log in.

A good supplement is training and information for users on how to handle and protect access-giving factors, so that the user is aware that they are still responsible for actions performed during login.

## WHEN IS THE MEASURE NECESSARY?

This generally follows from Article 5(1)(f) GDPR that personal data must be processed in a way that ensures protection against unauthorized or illegal processing. A risk assessment according to Article 32 GDPR will show which measures are relevant, as risks and opportunities are very dependent on the specific circumstances. As seen from the above, the use of anonymous login can increase the likelihood of deliberate misuse, lack of sense of responsibility and other things that result in unauthorized/illegal processing of data.

## Measure:

### Avoid copying access rights without actively taking a stand

### WHAT RISKS ARE ADDRESSED?

It may be easier to create new users by copying access rights from one user (who already has those rights) to the new user. However, this will entail the following risks:

- If there are errors in the access rights that are copied, e.g., accesses that should have been closed earlier, then the error will be copied to another user.
- The authorizing officer may not be aware of what is being copied, and thus does not actively decide whether it is necessary to copy all.
- Access rights for the existing user may change between the time of the authorisation manager's approval and the time of the copying of access rights, and thus doubts may arise as to what was approved. Thus, doubts may arise as to whether the user administrator has processed the task correctly or which access rights the authorisation manager has actually approved to be copied.
- As the person responsible for authorisation does not specifically state which access rights are to be granted, it is unclear what the person responsible for authorisation can subsequently be held accountable for if more access rights than necessary are granted and these are misused.

By rigorously managing the authorisation process and actively considering access rights, these risks can be minimised. In other words, this is a preventive measure that can minimise the likelihood of incorrect access rights.

### WHAT MEASURES CAN BE CONSIDERED?

Use an allocation procedure whereby the user's access rights are "built from scratch" and copying of access rights is not accepted. Alternatively, a controlled copying of access rights can be carried out, considering the above-mentioned risks, e.g., by considering each individual right in a form for each user, which can be signed by the person responsible for authorisation. The use of a form also ensures documentation, and the process promotes accountability on the part of the person responsible for authorisation.

See also the measure Documentation of authorisations.

## WHEN IS THE MEASURE NECESSARY?

Article 5(1)(f) of the GDPR is about the integrity and confidentiality of personal data. The fewer people have access to personal data, the more the risk that some of these users can pose through accidental or malicious actions is reduced. The less the individual user has access to, the less the potential consequence if some of these users do damage to data through accidental or malicious actions. At the same time, this also has a protective effect in relation to cyber threats, as a hacker often operates through access rights in compromised user accounts, and fewer rights thus give the hacker fewer opportunities. Access rights must therefore be limited as much as possible.

## Measure:

### Logging of users' use of personal data

### WHAT RISKS ARE ADDRESSED?

One of the purposes of logging is to enable investigation of past events in IT systems. For example, the log can show what actions users have performed in an IT system, but also what the IT system has done. In some cases, logs can also be used to detect ongoing incidents and thus possibly limit damage by detecting and stopping unauthorised actions. If users are aware that their use of personal data in IT systems is logged and analysed, it can help counteract deliberate misuse such as snooping. See also the measures Sampling logs of users' use of personal data and Awareness. Depending on the circumstances, this is:

- a *preventive measure* which can reduce the *likelihood* of abuse of access rights and,
- a *detection* and *corrective* measure if the log is actively used in connection with detecting and stopping an ongoing incident.

### WHAT MEASURES CAN BE CONSIDERED?

IT systems are developed and set up to log all uses of personal data by users, including reading, adding, searching (possibly search criteria), modifying, extracting and deleting - regardless of how the use of personal data is performed by the user. Relevant IT systems are developed/adapted to enable this logging.

IT systems are developed to be able to store log data for a specific period of time, e.g. the last x months. Enabling automatic deletion of logs is important for the data minimisation principle in Article 5(1)(c) of the GDPR.

The retention time of the log is set according to its purpose, so if a log is to be used to track abuse, it may be appropriate to set the retention time according to how often access rights are checked (see Periodic checks of the timeliness of access rights). Finding errors in these rights may trigger a need to review logs for at least the period since the previous check, as this will be the period during which the incorrect rights existed and could be misused. However, the need to investigate cyber-attacks may require a longer retention time, and the same applies to logs that are stored in connection with the investigation of a specific incident or suspected misuse.

Logs are stored in a location where they are protected in terms of confidentiality, integrity and availability. For example, a log server may be established that collects copies of logs from various IT systems. Procedures ensure that people with privileged access to these IT systems do not also

have access to the log server's copy of the logs. The log server is also specifically protected against cyber-attacks that can affect the IT systems.

It is ensured that it becomes possible for the data controller to obtain logs from data processors without major difficulty or expense.

Ensure accessible guidance on how to interpret logs and test the interpretation by using the guidance. This can be done, for example, by a blind test where one person performs/documents actions and another person uses the guidance to interpret the log, and then the two people's perceptions of what happened are compared.

The log is effectively tested. If there are multiple methods of viewing data, it is tested that this is logged regardless of which method is used.

It is checked whether logs are still being logged as expected and that log data is stored long enough and can be interpreted with the current guidance or an associated IT system. It is therefore a test of an established measure, cf. Article 32(1)(d) of the GDPR. The check is carried out during system changes as part of change management, but also possibly in between if there is a long time between system changes. See the Change Management measure.

If possible, the log is set up in a way that makes it possible to target samples of users' use of data for the purpose of checking use for work purposes. In this way, the logging will support the random checks, so that random checks can focus on uses that may be in violation of internal guidelines or be tantamount to snooping.

For direct physical access to registers with personal data, the log in the physical access system is also covered by the above measures.

If logs are to have a preventive effect and thus be a *preventive* measure, it requires that users have been made aware that misuse can be detected (via logs) and sanctioned. It also assumes that all actions can be traced to a single natural person, which is why the measures Avoid unnecessary use of multi-user accounts and Awareness must also be considered.

Logging is activated at the latest when the IT system is commissioned.

## WHEN IS THE MEASURE NECESSARY?

It is primarily a risk assessment in accordance with Article 32 of the GDPR that must show which measures are relevant, as risks are highly dependent on which processing of personal data takes place in different IT systems, as well as what preventive effect can be expected from users knowing that their actions are logged and can be investigated retrospectively.

In general, it can be said that the use of IT systems that contain many people's data is more risky because there is a greater possibility of misuse, and the more people who have access, the greater

the likelihood that someone may misuse the access, e.g. for private purposes or purposes that are not specifically work-related. However, the risk assessment must consider risks to confidentiality, integrity and availability, so other aspects may also necessitate logging.

Article 25 of the Regulation: When developing or acquiring new IT systems or developing/modifying existing IT systems, data protection must be incorporated into the design and default settings. To be able to log uses of personal data, the functionality must be built into the IT system. This includes the ability to store the log in a secure location where it is extra protected from being accessed/manipulated by users or hackers. The default setting should be that logging is enabled by default.

Logging the use of confidential and sensitive personal data has been a requirement for public authorities for many years. For state authorities, logging is required in the minimum technical requirements for state authorities.

In general, it is recommended to look at logging more broadly, so that logging is ensured both in relation to the above and in relation to the threats. the above and in relation to the threats that the Centre for Cyber Security focuses on through their recommendations on logging.

See also guidance on unauthorised access

## Measure:

### Logging of user administrator actions

### WHAT RISKS ARE ADDRESSED?

This measure has essentially the same purpose as the Logging of users' uses of personal data measure, but the requirements for the content of the log may be different because the focus must be on spotting misuse of user administrator access rights.

Checking the actions of a user administrator may have a different focus and frequency than checking the actions of other users. About random checks, see the description of measures under the measure Sampling in the log of users' use of personal data.

### WHAT MEASURES CAN BE CONSIDERED?

See the description of the measure Logging of user's use of personal data.

### WHEN IS THE MEASURE NECESSARY?

Same as the Logging of users' use of personal data measure. As the user administrator can typically give others and possibly themselves access to multiple IT systems, there is a particularly good reason to ensure control of this person's actions.

Article 25 of the GDPR: When developing or acquiring new IT systems or developing/modifying existing IT systems, data protection must be incorporated into the design and default settings. In order to be able to log the user administrator's actions, the functionality must be built into the IT system used for user administration, including in particular the functionality that the log must be able to be stored in a secure location where the user administrator cannot access / manipulate it via their privileged access rights.

## Measure:

### Minimizing the number of authorization officers and user administrators

### WHAT RISKS ARE ADDRESSED?

Access rights that are more extensive than necessary can pose an unnecessary risk of *loss of confidentiality, integrity and availability* through mishandling or outright misuse. By limiting the number of people who can grant access rights, the likelihood of errors and misuse is minimised. In other words, it is a *preventive* measure that can reduce the *likelihood* of erroneous or inconsistent granting of access rights.

The measure can also reduce the risk of external cyberattacks because it is less likely that compromising a random user's log-in will immediately allow them to control access rights to one or more IT systems. The measure is therefore also relevant in terms of mitigating the *impact* of misuse of authorised users' access rights.

### WHAT MEASURES CAN BE CONSIDERED?

Designate as few authorisation managers as possible.

Limit the organisational function responsible for user administration to as few people as possible. This can be difficult if user administrators are scattered throughout the organisation, which is why simultaneous implementation of the Centralised Rights Management measure will strengthen the overall preventive effect.

### WHEN IS THE MEASURE NECESSARY?

Article 5(1)(f) of the GDPR is about the integrity and confidentiality of personal data. The less an individual user can do with the data they have access to, the less the potential impact if some of these users compromise the integrity and confidentiality of data through unintentional or malicious actions. This also has a protective effect against cyber threats, as a hacker often operates through access rights in compromised user accounts, and fewer rights limit the hacker's options. Therefore, access rights must be limited as much as possible - and it must be limited who can grant new access rights.

The controller's assessment of the risk according to Article 32 of the Regulation can show which measures are relevant. For example, in the case of a two-person organisation, it may be necessary for both to be able to manage access rights without significantly increasing the risk of abuse, etc.

## Measure:

### Minimizing privileged access rights

### WHAT RISKS ARE ADDRESSED?

A typical hacker attack often includes the hacker acquiring more access rights, as this provides more options in the IT systems than a regular user's access rights. If the hacker is able to utilise a user account with privileged access rights, this is usually more problematic. Minimising the use of privileged access rights makes this harder to achieve. This is a preventative measure that can minimise the consequences if an attacker succeeds in taking over a user account.

### WHAT MEASURES CAN BE CONSIDERED?

The challenge is that someone always needs to have privileged access rights. So, in addition to limiting who has these privileges, you can also give the same user two user accounts - one regular with regular privileges and one with more privileges. By only using the privileged user account when absolutely necessary, you limit its exposure - but not if the employee will be using this account most of the time. The split into two accounts can also have the positive effect of making the user more aware of when they are working with access rights that can cause more damage (if mistakes are made). The split may not necessarily make sense in small organisations or if the specific employee only performs tasks that require the privileged access.

User administrator access is considered privileged access as it can be abused more than normal user accounts. Other types of privileged access are used for IT operations, such as direct access to a database, known as "SQL access". This can allow direct manipulation of the database - i.e. bypassing any access restrictions and security features normally found in applications that lie between the user and the database. This type of access is very risky and is only used under the following conditions:

- Granted only when absolutely necessary (time-limited).
- Only granted to people with IT operational tasks and the right competences.
- Only granted after some form of security clearance and possibly subject to a clean criminal record.
- Usage is logged and the log is stored in a place where it cannot be accessed by those using the access.

## WHEN IS THE MEASURE NECESSARY?

It is primarily a risk assessment according to Article 32 of the GDPR that will show which measures are relevant, as risks are highly dependent on the damage the user can do with privileged access rights. At the same time, this also has a protective effect against cyber threats, as a hacker often operates through access rights in compromised user accounts, and fewer rights give the hacker fewer options.

For state authorities: See claim # 6 i the minimum technical requirements for state authorities.

## Measure:

### Periodic control of the timeliness of access rights

### WHAT RISKS ARE ADDRESSED?

Entitlement management is a process that usually involves multiple people and mistakes can happen. There can also be a lack of focus on closing unnecessary access / access rights. An access rights audit can detect such errors that may otherwise exist for years. This is a *corrective* measure that can reduce the *likelihood* of misuse of unnecessary access rights.

### WHAT MEASURES CAN BE CONSIDERED?

A check may include one or more of the following investigations:

- Whether the access rights actually established are covered by a current, documented authorisation.
- Whether access should have been closed previously due to a time-limited / expired authorisation, resignation, leave of absence or other reasons.
- Whether authorisations are current - i.e., whether all approvals of access rights are necessary and based on a work-related need.
- Whether there are user accounts that are no longer used by the authorised user ("ghost accounts") and should therefore be closed.

The options and what is easiest depends on the IT systems in use. Access rights are checked against a credible, up-to-date source. Typically, this is an HR system that shows who is currently employed and what position they hold. If the organisation uses role-based access rights, the record in the HR system can very accurately indicate who should have access to what and which accesses should be closed.

"Controllers" with different roles (general manager, IT security manager, system owner, etc.) have different interests, and this must be taken into account when placing and explaining the control task to the controller. If the manager has to control access rights for their own employees, this manager may focus more on whether the necessary rights have been established than whether some users have too many rights.

The focus of a check can also be on saving money on user licences, which can remove unnecessary access rights, but it is still not a focus on whether the rights are necessary to fulfil a *work-related need*.

The frequency of the above-mentioned checks is adjusted depending on what problems the check reveals. If the check shows that errors are rare, fewer checks may be sufficient going forward. If, on the other hand, the check reveals many errors, the frequency or scope may need to be increased. Many errors may also indicate that other measures / processes are not working optimally. In this case, it may be more relevant to try to correct the day-to-day management of access rights rather than increasing the frequency of checks.

## WHEN IS THE MEASURE NECESSARY?

The Danish Data Protection Authority has stated that it is the Authority's view that the requirement for appropriate security in Article 32(1) of the GDPR will normally imply that the data controller continuously checks whether access rights to IT systems are limited to the personal data that are necessary and relevant to the work-related needs of the user in question.

This is because no matter how stringently access rights are managed, there are many places where things can go wrong in such a process that often involves many people. Therefore, there are likely to be errors that are only discovered through periodic checks.

## Measure:

### Pseudonymization and anonymization

#### WHAT RISKS ARE ADDRESSED?

Data that is anonymised is not subject to data protection rules or the resulting personal data security requirements. Anonymisation is a process that ensures that data cannot be linked to a natural person.

Pseudonymised personal data is data that can only be attributed to a natural person through the use of additional information, but where access to this additional information is highly restricted. Pseudonymisation can be used, for example, if some users need to use a dataset without being able to identify individuals in that dataset. The additional information that makes it possible to identify the individuals in the dataset can be found, for example, in another IT system to which the same users do not have access.

A user who only has access to anonymised data does not have access to personal data. A user who only has access to pseudonymised data will not be able to link it to a natural person (with their access rights). This is a *preventive* measure that can reduce the *consequences* of misuse of user accounts, whether the misuse is carried out by the authorised user or a hacker who takes over the user's access rights.

#### WHAT MEASURES CAN BE CONSIDERED?

The possibilities for implementing either anonymisation or pseudonymisation depend on the IT systems and the tasks performed in the specific organisation. True anonymisation and pseudonymisation are difficult processes that require an understanding of how individuals in a dataset can be identified.

#### WHEN IS THE MEASURE NECESSARY?

According to Article 32 of the GDPR that must show which measures are relevant, and the same article also mentions pseudonymisation as a potentially relevant measure. Note that both pseudonymisation and anonymisation are measures that are relevant in relation to the data minimisation principle in Article 5(1)(c) of the GDPR.

Article 25 of the GDPR: When developing or acquiring new IT systems or developing / modifying existing IT systems, data protection must be incorporated into the design and default settings. The possibility of either pseudonymisation or anonymisation requires that it is considered in the design

of the IT system and that it works with the employees' work tasks. Default settings can, among other things, allow pseudonymisation to happen automatically, e.g. based on how old the data is or the end of a customer relationship.

About pseudonymisation and anonymisation: What is personal data?

On what it takes to ensure effective anonymisation in a dataset: Article 29 Working Party working paper 216, "Opinion 05/2014 on Anonymisation Techniques"

## Measure:

### Role-based access rights

#### WHAT RISKS ARE ADDRESSED?

In larger organisations with many IT systems, assessing which access rights are appropriate can be a complex task. This increases the likelihood of errors when establishing rights. Role-based access assignment makes it easier for the authorisation manager to assess and approve access requests because it doesn't require an understanding of the access needs of each IT system, just knowledge of the users' roles / tasks. This makes the task easier for all parties involved, thereby minimising the likelihood of errors. In other words, it is a *preventative* measure that can minimise the *likelihood* of errors when assigning rights.

#### WHAT MEASURES CAN BE CONSIDERED?

Access rights are grouped based on the users' roles / tasks so that they cover the most typical work-related needs in relation to the individual work function, such as HR employee, bookkeeper, customer support, etc. This can also facilitate the task of defining access rights across IT systems.

#### WHEN IS THE MEASURE NECESSARY?

The need depends on the complexity of your IT environment. Therefore, it is a risk assessment according to Article 32 of the GDPR that will show which measures are relevant.

Article 25 of the GDPR: When developing or acquiring new IT systems or developing/modifying existing IT systems, data protection must be incorporated into the design and default settings. The possibility of simplifying rights assignment may depend on the design of the IT systems.

## Measure:

### Correlation between user competences, access rights and tasks

### WHAT RISKS ARE ADDRESSED?

Incorrect handling of data can lead to unintentional security breaches, such as the publication or disclosure of personal data that should have been omitted. The risk can be prevented by ensuring that each user has the necessary skills to use their authorisation and handle data correctly. This is a preventive measure that minimises the likelihood of data handling errors.

Many security breaches happen to users who use IT on a daily basis and therefore feel that they understand the technology, but still make mistakes. In some cases, this is because the user's focus is not on security, or because secure data handling requires a specialised understanding of IT - a different understanding than that required to perform the user's tasks. In some cases, security breaches are directly caused by a lack of understanding of the difference between the physical and electronic world, for example, if the user believes that data has been effectively removed from a document if the data is not immediately visible (on the computer screen).

### WHAT MEASURES CAN BE CONSIDERED?

When approving new access, there is a procedure in place to ensure that the employee in question has the necessary competences to handle data securely to avoid security breaches as much as possible. It's about avoiding giving users room to manoeuvre (via access rights) that is outside of their competencies and focus area.

Here are some examples where user access is considered in conjunction with the right competences.

- Access is not granted until the employee has the necessary competences. If access is already established, the employee is given the right competences before the task needs to be completed.
- Access rights to publish data on a website are only granted to employees for whom this task is a main area of work, and only after training on how to find and filter out personal data that may be stored in metadata in a document, in a dataset behind a graph in a presentation or in hidden cells in a spreadsheet. Tools and skills that enable them to remove data (not just hide it) and understand when data is anonymised may also be relevant.
- Electronic processing of access requests is only carried out by employees who have been provided with tools and competences that enable them to effectively remove data (not just hide it) and after training on relevant legal requirements on the scope of access.

- Personal data is only sent outside the organisation by employees who have been trained in the requirements for (secure) transmission. If possible, they have also been given tools that make it easy to send data securely.
- Journalising documents / letters that are automatically published at the same time is done by a small number of employees for whom this task is their main area of work. If there is automatic publication of documents in the journaling system, the employee is also trained on how it works.
- Some access rights may involve a higher risk than others. An employee with read access to data can compromise the confidentiality of data by passing it on to unauthorised persons. The ability to delete data carries an additional risk: the risk of data being inaccessible if, for example, the employee accidentally deletes the wrong data. The ability to delete data may also be linked to legal requirements, such as the rules of public administration, which may prohibit deletion in certain contexts. Such access rights are reserved for employees who have received training on relevant risks and / or legal requirements and for whom this task is their main area of work.

## WHEN IS THE MEASURE NECESSARY?

It is primarily a risk assessment according to Article 32 of the GDPR that will show which measures are relevant, as specific risks are highly dependent on whether there are functions / tasks in the organisation where a lack of competencies can actually pose a risk.

See the Awareness measure to select additional relevant information to be provided at the time of employment or when changing access rights.

## Measure:

### Samples in the log of users' use of personal data

### WHAT RISKS ARE ADDRESSED?

If users are aware that the use of the systems is being monitored, it may discourage misuse. Used in the right way, it is therefore a *preventive* and possibly also a *detection* measure that can reduce the *likelihood* of access rights being misused. Of course, this assumes that all actions can be traced to a single natural person, which is why the Avoid unnecessary use of multi-user accounts measure is also relevant.

The control measure may be particularly relevant in situations where access rights cannot be limited very much and where users must necessarily have broad access to a lot of personal data as part of their work, and where there may therefore be a particular risk that someone is tempted to use their access without it being specifically work-related.

### WHAT MEASURES CAN BE CONSIDERED?

Sampling of logs is carried out according to a fixed procedure, without the sampling being predictable for users.

The preventive effect requires that users are aware of the control measure, see the Awareness measure for more details.

It can be an advantage if the sample relates to relatively recent use, so that the user can reasonably be expected to be able to account for their treatment.

What the size of the sample should be is a concrete judgement. For example, if it is possible to automatically filter out a large number of entries in the data as being work-related (e.g. due to a known customer relationship, work area, therapist / patient relationship), then the sample of the remaining entries can be more limited or targeted than if the sample were to cover all entries.

Consider the need to establish alerts (e.g. based on log data) that are automatically triggered by suspicious activity. This can supplement or replace more random sampling.

Continuous random sampling also serves as a check that logs are still being logged as expected and that log data is stored long enough and can be interpreted with the current guidance. It is therefore also a test of an established measure and thus covered by Article 32(1)(d) of the GDPR. See the measure Logging of users' use of personal data.

## WHEN IS THE MEASURE NECESSARY?

It is primarily a risk assessment in accordance with Article 32 of the GDPR that must show how the random checks should be organised, including scope and frequency. This is because the risk depends on what processing of personal data takes place in different IT systems, as well as who and how many people have access.

In the case of broad access, i.e. where users have access to a large amount of sensitive personal data and / or access to data on many individuals, random checks every six months will often be necessary.

## Measure:

### Control of physical access

### WHAT RISKS ARE ADDRESSED?

Physical access restrictions can complement electronic data access restrictions, but in some cases the physical access restriction is the only prevention of unauthorised access to personal data. This is a parallel to an electronic login to IT systems or data media. It is a controlled restriction of access and thus a *preventive* measure that can minimise the *consequences* if user access is misused or abused.

The requirements for gaining electronic access to an IT system may be lower within a physical setting (e.g., an office building) than outside. A login may therefore be more complicated when a user uses remote access than when the same user logs in from an office workplace. Alternatively, remote access may be more limited.

Furthermore, there may be electronic accesses that, for security reasons, are only possible within a certain physical framework. Therefore, physical access rights can be an important part of protecting personal data - both those stored electronically and those on paper.

### WHAT MEASURES CAN BE CONSIDERED?

The following basically relates to protecting the confidentiality of data. Protecting integrity or availability may require significantly different measures, such as backup in the event of theft of IT equipment through compromised physical access.

Reception staff can stop unauthorised persons, and receptionists are instructed on how to react to people who do not normally have access (people claiming to have an errand as craftsmen, IT supporters, etc.), to what extent people should be identified, whether they should be escorted in, etc. Guest access through a reception desk is registered.

If reception staff cannot be expected to know all employees, it is probably safer to use personalised access media such as electronic access cards combined with a personal code. The card and code must be assigned, registered and blocked according to the same principles as the other rights management used for user IDs and passwords for logging in to IT systems.

If the organisation has premises with physical access to an IT environment (junction boxes and machine rooms), this access often involves the possibility of bypassing the electronic access restriction and thus the electronic rights management. Such premises need to have a special physical restriction and consider burglar-proof doors, automatic door closers with failure to close

alarms, secure key systems (tamper-proof, copy-protected), alarms, motion sensors, seismic detectors, etc.

Access to physical documents in offices, for example, can be restricted by security cabinets (safes) attached to a fixed part of the building. The key / code to the cabinet is managed according to the same principles as electronic access control. Safes are available in different "classes" that define their resistance to burglary - i.e. how difficult it is to break into the safe - and this must be adapted to how long it can take before an alarm / guard can be expected to interrupt the thief in his work.

Printers are placed where only employees have access, and in addition to this, solutions can be used that only print when the right user is at the printer (also known as "Follow Me Printing").

Physical access management is coordinated with other possible measures to prevent circumvention of physical access restrictions, such as guards, reinforced doors, intruder alarms, motion sensors, door lock failure alarms, personal locks, etc.

## WHEN IS THE MEASURE NECESSARY?

It is primarily a risk assessment according to Article 32 of the GDPR that must show which measures are relevant, as risks and opportunities are highly dependent on the specific circumstances.

It is largely an interaction between measures that creates an adequate level of security. Measures such as encryption of data media can drastically reduce the need for physical security in the office and home office. On the other hand, encrypting servers can be complicated and increase the risk of data unavailability and data loss, which is why physical security is prioritised over server encryption.

Article 25 of the Regulation: When developing or acquiring new IT systems or developing/modifying existing IT systems, data protection must be incorporated into the design and default settings. IT systems for e.g. access cards must therefore also be selected according to whether they can minimise access to personal data, e.g. by the IT system being able to differentiate between access to the machine room (server room), crossbar (network connections), office, customer service area, printer room, file archive, goods reception, etc.

See also: Guidance on unauthorised access

## Measure:

### Adaptation of access rights when changing the employment relationship

### WHAT RISKS ARE ADDRESSED?

When there are changes in employment, many changes must take place, and some of these directly or indirectly concern the employee's access to personal data. When access to IT systems is no longer needed, they must be closed, but this can be forgotten giving the user access for longer than necessary. More access provides a larger "attack surface" for malicious actors – they have, so to speak, more bricks to build their attacks with. Accesses that are no longer necessary therefore pose an unnecessary risk. Especially when employees are released, there may be a risk of misuse of access if these are not closed immediately. It is therefore a *preventive* measure which can reduce the *likelihood* that there are unnecessary access rights in the IT system which are misused.

A user account that is no longer used by the rightful user is also called a "ghost account." Even if the rightful user is prevented from using the account, for example by blocking the account in Active Directory, the access may still be misused. By shutting down such user accounts, the attack surface is reduced, as hackers are prevented from abusing a "ghost account" to gain access rights. Abuse of "ghost accounts" may also take place for a longer period of time without being detected, than in the case of abuse of the accounts that are still used by the rightful user.

### WHAT MEASURES CAN BE CONSIDERED?

Procedures or techniques are set up in such a way that the organization is forced to react when there are changes in employment conditions, such as employment, changed work tasks, leave, resignation, layoff, long-term illness, and death. Changes in employment conditions can trigger a notification, e.g., via an HR system. Alternatively, a fixed procedure can be established, meaning that unnecessary access rights are terminated. The process must ensure the same high focus on the termination of existing rights as on the creation of new ones.

It is ensured that the right employee receives information about the change to avoid situations where access remains open after employee resignation.

Some changes in employment conditions require that a time be set in advance for when a flag must be "raised" and a special process must be started - this applies, for example, if a security clearance automatically expires after x years with the consequent lack of approval for to access certain specially classified data.

Leave, maternity leave, sick leave etc. are situations where access must probably be closed, but as there is also a need to retain employees, closure takes place in a different way than in the case of resignations. For example, employees' access to the intranet can be maintained because information about social activities and information about the development of the workplace is shared here. In this way, the absent employee can still feel like part of the workplace. At the same time, employees' access to subject systems is closed or temporarily deactivated.

With internal rotation, tasks can be changed gradually. In this situation, a procedure or automation is ensured which causes accesses to be closed when they are no longer needed.

Finally, a special procedure is established for the peripheral/external systems which cannot be closed through a centralized user administration unit.

Consider the following *when access rights need to be removed or changed*:

- The employee must even close access in external IT systems, which it would otherwise be more difficult for others to close after resignation or transfer to another position.
- Employees with administrative rights must transfer these to another employee yourself.
- Deletion of data on PC / smartphone before delivery and possibly resetting or providing a code so that equipment can be reused.
- Cleaning up e-mail accounts, network drives, and especially in places where only this employee had access, or cleaning up private data so that the contents of the account can be made available to others after the resignation.
- Closing access to IT systems, function mailboxes and external IT systems.
- Inclusion of ID cards, key fobs, keys to doors / mailboxes / racks /..., access tokens, PC, smartphone, USB keys, hard drives, physical documents, etc.
- Changing codes that are shared between multiple users (multi-user accounts).
- Blocking access via key fobs, access cards, physical access / alarm panels, cabinates / safes.
- Replacement / recoding of lock cylinders (if the key is not copy-protected).
- Blocking remote access to IT systems.
- Blocking access with certificates and possibly the certificates themselves (MitID Erhverv, certificates attached to hardware, ...).
- Cancellation of telephone subscription and internet subscription through the company. If the employee is allowed to keep the phone, special attention is paid to the fact that there is no company data on the phone and that synchronization of data (typically calendar appointments and e-mails) is stopped.
- Deletion of employee data that is no longer necessary, e.g., photo used for ID card or phone book information on the intranet.
- Internal contact lists are updated, and external partners are informed of changes in contact points (customers, security company, craftsmen, ...), especially if the employee can continue to use the telephone number after resignation.
- Revision of emergency organisation, system ownership, etc. if the employee was covered by this.

- Investigating whether inappropriate reliance on individuals occurs when access rights are removed or changed.

## WHEN IS THE MEASURE NECESSARY?

It follows from Article 5(1)(f) of the GDPR that sufficient security must be ensured when processing personal data, including protection against unauthorized and illegal processing. Closing access reduces the possibility of unauthorized and illegal processing, which can be particularly important in situations where an employee is dismissed. In very special situations, a risk assessment will be able to show that the measure is not necessary if, for example, access is only to publicly available personal data, and misuse in the form of changing/deleting this information cannot harm the data subjects.

## Measure:

### Change Management

### WHAT RISKS ARE ADDRESSED?

In the event of changes in IT environments, software, the organization, business processes and proceedings, etc. errors may occur. Errors can also occur in places in an IT environment that are not directly affected by a given change, because the changes trigger derivative errors in associated systems, or errors can occur as a result of proceedings not being adapted to planned changes in an IT environment.

Good change management implies that such changes are managed according to established principles. What change management actually entails can vary from situation to situation - the key is to have fixed procedures to handle and assess the consequences of planned changes before they are implemented. You try to anticipate errors both to avoid them, but also to have a plan to deal with the consequences if errors occur in connection with the change. This is therefore a measure with many facets. How it affects risks depends on which part of change management you are talking about.

Errors can, for example, occur if existing measures are not ensured to be continued when the server is replaced, for example the continuation of an access restriction on a folder on a network drive that is moved to another server.

Other errors can arise through integration between IT systems and automated processes. When initiating data transfers between IT systems, it must be ensured, for example, that marking regarding changed names/name protection is included, so that information about protected names is not inadvertently exposed in another IT system.

Below are a number of examples where better change management could have made a difference:

- In connection with moving to a municipality, an enrolment letter is sent from the school to both parents. Broadcasting is done automatically to both parents, even if the child lives with one parent at a protected residential address, but the residential address is not omitted, whereby information about a protected address is inadvertently passed on. This is because, when developing a new IT system, sufficient consideration has not been given to which personal data is processed in the IT system and how this information may be used in the new IT system. The sending of letters has been automated without taking into account individual problematic circumstances surrounding the protection of some of the processed personal data.
- Non-cohabiting parents with joint custody are given the opportunity to log on to a self-service solution so that both parents can access letters regarding the joint child. It is not

considered that information about protected address, which is on letters, cannot be accessed by the other parent.

- The municipality has information that one parent has a restraining order against visiting the other parent and that the child's address is protected. Nevertheless, an SMS is sent to both parents with information on where and when the common child has an appointment at a dental clinic. The error is due to a failure to update data between IT systems.
- A form for changing schools allows you to enter a social security number, after which the IT system automatically sends a receipt to both parents with an address. The system does not take address protection into account, which is why one parent can unjustifiably obtain the other parent's protected address by entering the other parent's social security number in the form.
- A school sends an SMS to a child's biological parents about a school event, even if the biological parents are not allowed to know the child's whereabouts. This gives the parents information about which school the child attends. Part of the problem is slow updating between IT systems and failure to consider update frequencies. There is a lack of overview of which systems receive which data and at what speed.
- A parent without parental authority receives an SMS with the address of the child's school, even if the child's location is protected. It was due to an error in setting up an IT system, as an integration between IT systems was carried out without the necessary testing.
- Roll call in class (absence registration) takes place using a protected name, because data for the roll call does not come from one of the school systems where the name is replaced by an alias, but is instead obtained directly from CPR.
- Bad coding in the IT system means that the indication of address protection is not included when cases are sent from one authority to another. This entails a risk that the receiving authority will mistakenly hand over information about a protected address, for example when handing over documents in the case.

## WHAT MEASURES CAN BE CONSIDERED?

It is revealed which processing activities are affected by one or more planned changes in the IT environment. It is also uncovered whether the change can affect parts of the environment or associated processes and applications of the affected IT systems, which are not directly the subject of the change itself. In this way, it can be determined which parts must be tested in connection with the changes.

All probable error scenarios are ensured to be uncovered before implementing the change, just as the relevant error scenarios are tested to the extent necessary. All errors found are assessed based on possible risks to data subjects' rights and freedoms, and it is assessed - in particular by the DPO (if one has been appointed) - whether they mean that the change must be postponed until the error is corrected.

A check is launched to see if existing measures are continued in the event of a system change. Among other things the following:

- Tests are carried out which ensure that all control measures in an IT environment, which have been established throughout the life of the IT environment, are continued or replaced by something equivalent after a change.
- It is checked whether logging is taking place in the IT system that is to be changed. Such logging must be tested immediately after the change, so that it is ensured that logging is still carried out as expected and that log data is stored long enough and can be interpreted with the current guidance or an associated IT system. If this is not implemented, a system change can undermine measures such as Logging of users' uses of personal data and Logging of user administrator actions.
- It is checked whether the IT system to be changed includes areas with restricted access. If it does, measures are implemented to ensure that the current rights management is continued, discontinued or adapted to the extent necessary, and the access restrictions are tested immediately after the implementation of the changes.
- Rights management can take place within a very small group of employees who, for example, have chosen to restrict access to a folder on a server drive. It is important to uncover and take into account such decentralized rights management before the change to the IT system is started.
    - If RPA (Robotic Process Automation) or similar is used, it is checked that the robot user's access rights are still current or whether they need to be restricted.
    - If the change concerns direct access to databases, file stores and the like outside of usual applications with rights management, it must be ensured that the applicable rights management is not affected by the change. Especially when moving from test to production, this can be overlooked. Typically, at most the administrator and possibly service account could access a database directly.
- In the case of integration between IT systems, and especially where data is actively exchanged, the following is uncovered:
    - whether the update frequency is sufficient,
    - whether sufficient data is transferred,
    - whether the changes may have an impact on applicable legal requirements for the processing of data, such as whether data is used for unauthorized purposes, stored for longer than necessary, etc.
- Attention is paid to whether changes in the integration can lead to unintended changes in access rights, with the risk that, for example, more data can be accessed than should be, or data that is necessary to manage the handling of other data turns out to be missing. This could, for example, be a situation where an error is experienced on a communication connection to a data source, which is why you quickly switch to an alternative data source. However, the alternative source has outdated data, which means that outdated data is used in the automated processes.

## WHEN IS THE MEASURE NECESSARY?

It follows from Article 32(1)(b) of the GDPR that relevant measures to ensure a level of security appropriate to the assessed risks may include the ability to ensure continued confidentiality, integrity, availability and robustness of processing systems and services.

Change management is always relevant for changes in an IT environment, software, the organization, business processes, etc. - even if the development does not take place in-house. In the case of outsourced IT, requirements for change management can advantageously be included in IT contracts and data processing agreements. Change management can also be relevant for changes in procedures and organization.

Here are a few examples of scenarios where change management must be under control:

- If the organization – possibly in collaboration with a data processor - makes changes to IT systems, work procedures, etc., then Article 32(1)(b) of the GDPR is relevant, as any change in IT systems, work procedures, etc. may introduce errors that affect confidentiality, integrity, availability, or robustness.
- Changing an IT system can introduce errors if it causes work procedures to no longer fit the IT system. Conversely, changes in procedures must be made with an understanding of how the IT system works, so that it does not introduce errors.
- Changes in the organization can also introduce errors if new employees are assigned to a job for which they have not first been properly trained, or which is far from the employee's normal focus area - for example if a pedagogue is tasked with case management in an IT system, that is not intuitive, that the employee is not trained in, or that is not secured against user error.

The above shows that the development / change of both IT systems, procedures and organization must be done with a focus on processing security, and that the IT system, procedures and organization must fit together.  Article 25 of the GDPR aims to ensure data protection is thought into the design, and not only the design of IT systems, but also of the organization and in the organization's work processes / procedures.