GDPR

Studsvik

At Studsvik, we collect and process information about individuals (i.e. 'personal data') for business purposes, including employment and HR administration, provision of our services, marketing, business administration and because of regulatory obligations. This includes personal data relating to our staff, customers, suppliers and other third parties.

GDPR at Studsvik

Compliance with data protection law is essential to ensure that personal data remains safe, our business operations are secure, and the rights of individuals are respected. Studsvik is a controller under data protection law, meaning it decides how and why it uses personal data. This document explains our procedures for complying with data protection law in relation to personal data. It also sets out Employees of Studsvik's obligations whenever they are processing any personal data in the course of their employment.

This policy is supplemented by a guideline providing further procedures. This is of particular importance for employees who routinely handle personal data.

There will also be other policies which will impact personal data and data protection is dealt with.

This document does not give contractual rights to any Employees. It may be updated at any time.

Who does this Policy apply to?

This document applies to all Studsvik employees, workers, contractors, agency workers, consultants, interns, volunteers and directors (together referred to as 'Employees').

Who is responsible for data protection at Studsvik?

The Group Board is ultimately responsible for Studsvik's compliance with applicable data protection laws. The organization has not appointed a Data Protection Officer, instead,

a Data Protection Lead for the whole group, a role delegated to the CFO, is responsible for overseeing and advising Studsvik on and administering compliance with this document and data protection laws. Local Data Protection Representatives are also appointed country wise who can be accessed via the Data Protection Lead. The Local Data Protection Representative is to give advice and decide on exemptions from contracts with third party on disclosure of personal data, new/changed forms of collection of personal data or in connection with automated decision-making or profiling activities. The Local Data Protection Representative is further to receive and handle reporting of data protection breaches, be the recipient of and handle related reporting from employees in the event of requests, enquiries or complaints and be aware about the records of the personal data being kept. The local Data Protection Representatives reports directly to the Data Protection Lead for the group, which includes to keep the Data Protection Lead informed about deviations and engaged for decision-making when necessary. When processing personal data, roles and responsibilities may differ depending on the circumstances. In some cases, the organization acts as the data controller, determining the purposes and means of the processing. In other cases, it may act as a data processor, processing personal data on behalf of another controller and in accordance with that party's documented instructions.

In certain situations, two or more parties may jointly determine the purposes and means of the processing. In such cases, the parties act as jointly responsible controllers and define their respective responsibilities, in particular regarding transparency, data subject rights and compliance with applicable data protection requirements.

All Employees at Studsvik have a responsibility for ensuring that personal data is kept secure and processed in a lawful manner although certain Employees will have particular responsibilities, of which they will be aware and in respect of which they may receive specific instructions.

If in doubt about how personal data should be handled, or to raise any concerns or questions in relation to the operation (or suspected breaches) of this Document, you should seek advice from the local Data Protection Representative.

Contact details for the relevant Data Protection Representative are made available internally via the company intranet. External individuals may contact the organisation through the general contact channels, and their request will be forwarded to the appropriate Data Protection Representative without undue delay.

Why is data protection compliance important?

Data protection law in each country is regulated and enforced by a relevant governing body. Failure to comply with data protection law may expose Studsvik and, in some cases, individual Employees to serious legal liabilities. These can include criminal offences and fines of up to EUR20 million (approximately £18 million) or 4 % of total worldwide annual turnover, whichever is higher. In addition, an individual may seek damages from Studsvik in the courts if their rights are breached under data protection law. Breaches of data protection law can also lead to serious damage to the Studsvik brand and reputation.

In addition to the legal liabilities, failure to comply with your obligations under this Policy could lead to disciplinary action and, in serious cases, it could result in the termination of your employment.

What is personal data?

Personal data means any information relating to any living individual (also known as a 'data subject') who can be identified (directly or indirectly) in particular by reference to an identifier (e.g. name, employee number, email address, physical features). Relevant individuals can include colleagues, customers, members of the public, business contacts, etc. Personal data can be factual (e.g. contact details or date of birth), an opinion about a person's actions or behaviour, or information that may otherwise impact on that individual. It can be personal, or business related.

Personal data may be automated (e.g. electronic records such as computer files or in emails) or in manual records which are part of a filing system or are intended to form part of a filing system (e.g. structured paper files and archives).

What does 'processing' personal data mean?

'Processing' personal data means any activity that involves the use of personal data (e.g. obtaining, recording or holding the data, amending, retrieving, using, disclosing, sharing, erasing or destroying). It also includes sending or transferring personal data to third parties.

Data Protection Obligations

Studsvik is responsible for and must be able to demonstrate compliance with data protection laws. To ensure that Studsvik meets its responsibilities, it is essential that its Employees comply with applicable data protection law and any other Studsvik policies, guidelines or instructions relating to personal data when processing personal data in the course of their employment.

We have set out below the key obligations under data protection law and details of how Studsvik expects Employees to comply with these requirements.

Process personal data in a fair, lawful and transparent manner

Legal grounds for processing

Data protection law allows us to process personal data only where there are fair and legal grounds which justify using the information.

Examples of legal grounds for processing personal data include the following (at least one of these must be satisfied for each processing activity):

- complying with a legal obligation (e.g. health and safety or tax laws);
- entering into or performing a contract with the individual (e.g. an Employee's terms and conditions of employment, or a contract for services with an individual customer);
- acting in Studsvik's or a third party's legitimate interests (e.g. maintaining records of business activities, monitoring business productivity); and
- obtaining the consent of the individual (e.g. for sending direct marketing communications).

Where consent is relied upon, it must be freely given, specific, informed and unambiguous, and Studsvik must effectively demonstrate that consent has been given.

In line with local government body guidance regarding the employer / Employee relationship, Studsvik does not use consent as a legal ground for processing Employee data unless the data processing activities concerned are genuinely optional.

In most cases, consent is also not required for other standard business activities involving use of customer or supplier data, but it may be needed for activities which are not required to manage the main business relationship, such as direct marketing or combined business development activities. In this event, we should never assume that consent has been implied and always seek to obtain written consent e.g. in the instance of forwarding on a customer or supplier's CV or competence data.

Transparency

Data protection law also requires us to process personal data in a transparent manner by providing individuals with appropriate, clear and concise information about how we process their personal data.

We usually provide individuals with basic information about how we use their data on forms which collect data (such as application forms or website forms), and in longer privacy notices setting out details including: the types of personal data that we hold about them, how we use it, our legal grounds for processing the information, who we might share it with and how long we keep it for. For example, we provide information about our processing of Employees' personal data in the Studsvik Employee Privacy Notice.

We supplement these notices, where appropriate, with reminders or additional information at the time particular processing activities take place or become relevant for an individual (for example when they sign up for a new service or event).

In addition to personal data collected directly from the individual, we may also process personal data obtained from other sources.

Such personal data may originate from references, customers, public authorities, business partners, or other third parties, as well as from publicly available sources, including professional networks and similar platforms.

Personal data obtained from external sources is processed only for specific and legitimate purposes, is limited to what is necessary for those purposes, and is handled with appropriate technical and organizational measures to protect the data against unauthorized access, loss, or misuse.

Where required, we provide the individual with information about the processing of their personal data, including the type of data collected, the purpose of the processing, and their rights under applicable data protection legislation. This information is provided within a reasonable timeframe after the data has been obtained or, where applicable, at the latest when the personal data is first used or disclosed.

In certain situations, information may not be provided where this is permitted under applicable data protection law, for example where providing such information would be impossible or involve disproportionate effort.

What you as an Employee need to do:

By processing personal data only in accordance with your lawful job duties and Studsvik instructions, ordinarily, you will be processing personal data fairly and lawfully.

The standard privacy notices and statements that we issue, for example, to Employees, customers and the public, should normally be sufficient to ensure that individuals have appropriate information about how you are handling their personal data in the course of your employment. However, you should consider whether reminders or additional information may be appropriate at the time particular processing activities take place. This is particularly important if you think that individuals may need further assistance to understand clearly how their data will be used as part of such activities.

Any new forms which collect personal data and any proposed consent wording must be approved in advance by your local Data Protection Representative.

If you have any concerns about the legal grounds for processing personal data or if you are unsure whether individuals have been provided with appropriate information (in particular in relation to any new processing activities), please check with your local Data Protection Representative.

Take extra care when handling sensitive or special categories of personal data

Some categories of personal data are 'special' because they are particularly sensitive. These include information that reveals details of an individual's:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- sexual life or sexual orientation;
- biometric or genetic data (if used to identify that individual); and
- criminal offences or convictions.

Where special category personal data is concerned, data protection law requires us to have (as well as one of the legal grounds described in section "Legal grounds for processing"), an additional legal ground to justify using this sensitive information. The appropriate legal ground will depend on the circumstances.

Additional legal grounds for processing special category data include the following. Those marked with an asterisk (*) would be particularly relevant to processing Employees' special category personal data:

What you as an Employee need to do:

If you are handling special category personal data in the course of your employment, you need to take extra care regarding compliance with data protection law. In particular, try to ensure that:

- any processing activities are strictly in accordance with your lawful job duties and Studsvik instructions;
- there are appropriate legal grounds for processing the data (both basic grounds under section "Legal grounds for processing" and additional grounds under this section) which have been assessed for your specific activities;
- individuals have received adequate information regarding how their data is being handled. In some cases, an existing privacy notice may need to be supplemented with more specific information regarding special category data;
- you apply additional security and confidentiality measures, considering that the impact on individuals of loss or misuse of their special category data may be greater than with other types of data. See also section "Take appropriate steps to keep personal data secure" below; and
- if you are relying on consent as a legal ground for processing, you obtain advance approval of any consent wording from your local Data Protection Representative.

If you are routinely handling special category data as part of the requirements of your role and job duties, Studsvik will ordinarily have put in place procedures which ensure that your processing activities satisfy the requirements above.

However, if alternative circumstances apply (e.g. you are involved in a new project or updating an existing system which involves new types of processing of special category data), please contact your local Data Protection Representative to ensure that the correct compliance procedures are followed.

Similarly, if you have any concerns over the legal grounds that apply when you are processing special category data or the appropriate information to be provided to individuals, please get in touch with your local Data Protection Representative.

Only process data for specified, explicit and legitimate purposes

Studsvik will only process personal data in accordance with our legitimate purposes to carry out our business operations and to administer employment and other business relationships.

What you as an Employee need to do:

You must only use the personal data that you process in the course of your duties for Studsvik's legitimate and authorized purposes. You must not process personal data for any purposes which are unrelated to your job duties.

Processing personal data for any incompatible or unauthorized purposes could result in a breach of data protection law (e.g. using the company contacts database to find out a colleague's home address for private, non-work related purposes). This may have potentially damaging consequences for all parties concerned, including disciplinary action.

If you find that you need to process personal data for a different purpose from that for which it was originally collected, you must check whether the individuals have been informed and, if not, consider whether the additional purpose is legitimate (in the context of Studsvik's business activities) and compatible with the original purpose.

If you are unsure about whether the purposes for processing are legitimate, you should contact your local Data Protection Representative before going ahead with processing the data for the additional purpose.

Make sure that personal data is adequate, relevant and limited to what is necessary for your legitimate purposes

Data protection law requires us to ensure that, when we process personal data, it is adequate, relevant to our purposes and limited to what is necessary for those purposes (also known as 'data minimization'). In other words, we ask for the information we need for our legitimate business purposes, but we won't ask for more information than we need in order to carry out our business operations.

What you as an Employee need to do:

You should try to ensure that you only acquire and process the personal data that you actually need for Studsvik's legitimate and authorized purposes within the scope of your role.

You must ensure that you have sufficient personal data needed to be able to use it fairly and to consider all relevant details.

If you are creating forms that collect personal data, you should be able to justify why each specific category of data is being requested.

You must also comply with Studsvik's instructions about data retention and storage, ensuring that personal data is only kept for as long as it is needed for any intended purpose.

Keep personal data accurate and (where necessary) up-to-date

Studsvik must take steps to ensure that personal data is accurate and (where necessary) kept up-to-date. For example, we request that Employees provide us with any change in contact details or personal information via relevant local forms. We also take care that decisions impacting individuals are based on accurate and up-to-date information.

What you as an Employee need to do:

When you process individuals' personal data in the course of your employment, you must make reasonable efforts to be accurate and, where necessary, keep the relevant information updated.

When collecting any personal data, try to confirm its accuracy at the outset. If you subsequently discover any inaccuracies in the personal data that you are handling, these need to be corrected or deleted without delay.

Personal data should be held in as few places as possible to avoid the risk that duplicate copies are not updated and become out of sync. You should not create additional copies of personal data but should work from and update a single central copy where possible (in accordance with standard Studsvik procedures on retention and storage of records).

Keep personal data for no longer than is necessary for the identified purposes

Records containing personal data should only be kept for as long as they are needed for the identified purposes. Studsvik has in place data retention, storage and deletion policies and internal processes / guidelines regarding various types of company records and information that contain personal data.

We take appropriate steps to retain personal data only for so long as is necessary, considering the following criteria:

- the amount, nature, and sensitivity of the personal data;
- the risk of harm from unauthorized use or disclosure;
- the purposes for which we process the personal data and how long we need the particular data to achieve these purposes;
- how long the personal data is likely to remain accurate and up-to-date;
- for how long the personal data might be relevant to possible future legal claims; and
- any applicable legal, accounting, reporting or regulatory requirements that specify how long certain records must be kept.

What you as an Employee need to do:

Please familiarize yourself with our retention policies, processes, guidelines and instructions that are relevant to your job. Ensure that, where it falls within your responsibility, you destroy or erase all information that you no longer require in accordance with these.

If you are not sure what retention guidelines / instructions apply to you in your role, or you are unsure of how to apply them to a particular type or item of personal data, please contact your local Data Protection Representative.

Take appropriate steps to keep personal data secure

Keeping personal data safe and complying with Studsvik's security procedures to protect the confidentiality, integrity, availability and resilience of personal data is a key responsibility for Studsvik and its workforce.

Studsvik sets out in relevant local policies its arrangements for handling Confidentiality and Data Protection matters, which specifically sets out its organizational and technical security measures to protect information, including personal data.

The same goes for "Information Technology" arrangements, setting out protocols for Employees on use of technology and communications systems, which also help to ensure appropriate security of personal data stored or communicated using such systems.

We regularly evaluate and test the effectiveness of these measures to ensure the security of our personal data processing.

What you as an Employee need to do:

To assist Studsvik in maintaining data security and protecting the confidentiality and integrity of the personal data you handle in the course of your employment, we require you to comply with this Document and all other relevant local policies, as well as any Studsvik instructions regarding the processing and security of personal data. In particular, we require you to:

- save, store and communicate personal data only within or using authorized Studsvik information and communications systems. Restrict storage of personal data on personal devices or using personal communications facilities (or BYOD controls)
- use password-protected and encrypted software for

the transmission and receipt of emails and files in a secure cabinet within the relevant department
- never leave your laptop, other device or any hard copies of documents containing personal data in a public place
- take care when observing personal data in hard copy or on-screen that such information is not viewed by anyone who does not have the right to that information, especially if you are viewing the personal data in a public place
- when storing data on portable devices such as laptops, smartphones, or USB drives, ensure that the device is encrypted, and password protected
- ensure that information containing personal data is disposed of securely and permanently, using confidential waste disposal or shredding where necessary
- alert your local Data Protection Representative to any personal data breaches immediately (see below for further details about personal data breaches)
- ensure that any sharing or disclosure of personal data is permitted on appropriate legal grounds and, where necessary, safeguards are in place (see below for further details of safeguards regarding overseas transfers or if sharing personal data with third party service providers)

Take extra care when sharing or disclosing personal data

The sharing or disclosure of personal data is a type of processing, and therefore all the principles described in this Document need to be applied.

Internal data sharing

Studsvik ensures that personal data is only shared internally on a 'need to know' basis.

External data sharing

We will only share personal data with other third parties (including group entities) where we have a legitimate purpose, and an appropriate legal ground under data protection law which permits us to do so. Commonly, this could include situations where we are legally obliged to provide the information (e.g. relevant bodies for tax purposes) or where necessary to perform our contractual duties to individuals (e.g. provision of information to our occupational pension providers).

We may appoint third party service providers (known as processors) who will handle information on our behalf, for example to provide payroll, data storage or other technology services.

Studsvik remains responsible for ensuring that its processors comply with data protection law and this Document in their handling of personal data. We must assess and apply data protection and information security measures prior to and during the appointment of a processor. The extent of these measures will vary depending on the nature of the activities, but will include appropriate risk assessments and reviews, and contractual obligations. As part of the risk assessment process, situations may arise where the processing of personal data involves increased risks to individuals, for example when sensitive personal data is processed or when the nature, scope or purpose of the processing is likely to have a significant impact. In such cases, the relevant Data Protection Lead or Data Protection Representative assesses whether a data protection impact assessment needs to be conducted.

Details of the recipients or categories of recipients of personal data (including processors and other third parties) should be set out in privacy notices as described in section "Legal grounds for processing" above.

What you as an Employee need to do:

You may only share or disclose the personal data we hold internally with an Employee, agent or representative of Studsvik if the recipient has a job-related need to know the information.

You may only disclose the personal data we hold to service providers or other third parties (including group entities) where:

- there is a legitimate purpose and an appropriate legal ground for doing so (e.g. it is necessary for them to process the personal data in order to provide a service to us such as payroll, or if we are legally obliged to do so);
- the individuals whose personal data is being shared have been properly informed (e.g. in an appropriate privacy notice);
- if the disclosure is to a service provider, Studsvik has checked that adequate security and data protection measures are in place to protect the personal data concerned;
- the service provider or third party has signed up to a written contract, a data processing agreement, that contains the provisions required by relevant data protection law (unless your local Data Protection Representative has determined that this is not required in context); and
- the transfer complies with any overseas transfer restrictions, if applicable.

Routine disclosures of personal data to established recipients (e.g. payroll providers or group entities) which form a normal and regular part of your role and job duties will ordinarily satisfy the above requirements. You should always ensure you comply with any particular Studsvik instructions you are given. However, if you are in any doubt as to whether you can share personal data with anyone else, first contact your local Data Protection Representative.

Do not transfer personal data to another country unless there are appropriate safeguards in place (applicable to European group companies only)

An overseas transfer of personal data takes place when the data is transmitted or sent to, viewed, accessed or otherwise processed in, a different country. European Union data protection law restricts, in particular, personal data transfers to countries outside of the European Economic Area (EEA – this is the European Union plus Norway, Liechtenstein and Iceland), to ensure that the level of data protection afforded to individuals is not compromised (as the laws of such countries may not provide the same level of protection for personal data as within the EEA).

To ensure that data protection is not compromised when personal data is transferred to another country, Studsvik assesses the risks of any transfer of personal data outside of each country (taking into account the principles in this Document, as well as the restrictions on transfers outside the EEA) and puts in place additional appropriate safeguards where required.

For example, each European subsidiary currently sends personal data to the parent organization within the Studsvik Group on an as-required basis for group reporting. Subsidiaries may also occasionally send very basic personal data to other group companies (Germany, UK, Sweden and the USA), the purposes of which are limited to competence development and resource sharing, as well as business development activities. We may send competence information to external parties outside of the Studsvik group in pursuit of winning new business in markets we are not currently established. In all these instances, a minimum of two layers of security will be put in place to safeguard the data. These may include the examples set out in section "Take appropriate steps to keep personal data secure".

What you as an Employee need to do:

If you are required to transfer individuals' personal data outside of the EEA in the course of your employment, adequate safeguards will need to be in place. Where these overseas transfers are a normal part of your role and job duties, Studsvik's current safeguards are likely to provide the required levels of data protection.

However, if you are transferring personal data overseas in alternative circumstances (e.g. for new types of processing activities which haven't previously formed part of your job scope and activities, or to countries with which you haven't previously dealt) you should contact your local Data Protection Representative for further guidance before going ahead with the transfer.

Report any data protection breaches without delay

Studsvik takes any data protection breaches very seriously. These can include lost or mislaid equipment or data, use of inaccurate or excessive data, failure to address an individual's rights, accidental sending of data to the wrong person, unauthorized access to, use of or disclosure of data, deliberate attacks on Studsvik's systems or theft of records, and any equivalent breaches by Studsvik's service providers.

Where there has been a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to individuals' personal data, Studsvik will take immediate steps to identify, assess and address it, including containing the risks, remedying the breach, and notifying appropriate parties (see below). Each Studsvik subsidiary or legal entity sets out in relevant local policies its own arrangements for identifying, assessing and addressing security breaches.

If Studsvik discovers that there has been a personal data security breach that poses a risk to the rights and freedoms of individuals, we will report it to the local government body within 72 hours of discovery.

We also keep an internal record of all personal data breaches regardless of their effect and whether or not we report them to the local government body.

If a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken.

What you as an Employee need to do:

If you become aware of any breach (or suspected breach) of this Document (including, in particular any security breach), you must report it to your local Data Protection Representative immediately and take any other required steps in accordance with relevant local policies to ensure that the breach is effectively assessed and addressed, and that we comply with Studsvik's data breach reporting obligations.

Do not use profiling or automated decision-making unless you are authorized to do so

Profiling, or automated decision-making, occurs where an individual's personal data is processed and evaluated by automated means resulting in an important decision being taken in relation to that individual. This poses particular risks for individuals where a decision is based solely on that profiling or other automated processing.

One example of solely automated decision-making would be using an online psychometric test to automatically reject job applicants who do not meet a minimum pass mark (without any human oversight such as a review of the test results by a recruiting manager).

Data protection law prohibits decision-making based solely on profiling or other automated processing, except in very limited circumstances. In addition, where profiling or other automated decision-making is permitted, safeguards must be put in place and we must give individuals the opportunity to express their point of view and challenge the decision. We do not generally conduct profiling or other automated decision-making in respect of Employees, however Studsvik may on rare occasions use basic screening questions to automatically reject job applicants that do not hold the minimum requirements for a particular role. In this instance personal data is assessed for compliance with these requirements and appropriate safeguards are implemented on a case by case basis.

What you as an Employee need to do:

If you conduct profiling or other automated decision-making in the course of your role, you must familiarize yourself with and implement any applicable safeguards.

If you are proposing to undertake any new automated decision-making or profiling activities in the course of your employment, please contact your local Data Protection Representative, who will advise you whether it is permitted and about the safeguards you need to put in place.

Integrate data protection into operations

Data protection law requires Studsvik to build data protection considerations and security measures into all of our operations that involve the processing of personal data, particularly at the start of a new project or activity which may impact on the privacy of individuals. This involves taking into account various factors including:

- the risks (and their likelihood and severity) posed by the processing for the rights and freedoms of individuals;
- technological capabilities;
- the cost of implementation; and
- the nature, scope, context and purposes of the processing of personal data.

We also seek to assess data protection risks regularly throughout the lifecycle of any project or activity which involves the use of personal data.

What you as an Employee need to do:

If you are involved in the design or implementation of a new project or activity that involves processing personal data, you must give due consideration to all the principles of data protection set out in this document.

You should assist your local Data Protection Representative with regular reviews of projects or activities to ensure data protection risks continue to be addressed.

If you are involved in the design or implementation of a new project that involves processing personal data, you must check whether it is necessary to conduct a risk or compliance assessment by contacting your local Data Protection Representative. They will also be able to advise you on how we expect you to conduct, or otherwise contribute to, a risk assessment.

Individual rights and requests

Under data protection law, individuals have certain rights when it comes to how we handle their personal data. For example, an individual has the following rights:

- The right to make a 'subject access request'. This entitles an individual to receive a copy of the personal data we hold about them, together with information about how and why we process it and other rights which they have (as outlined below). This enables them, for example, to check we are lawfully processing their data and to correct any inaccuracies.
- The right to request that we correct incomplete or inaccurate personal data that we hold about them.
- The right to withdraw any consent which they have given.
- The right to request that we delete or remove personal data that we hold about them where there is no good reason for us continuing to process it. Individuals also have the right to ask us to delete or remove their personal data where they have exercised their right to object to processing (see below). While individuals have the right to request the erasure of their personal data, this right is not absolute, and personal data may need to be retained where necessary to comply with legal obligations, such as accounting or employment law, to establish, exercise or defend legal claims, or to meet product liability requirements.
- The right to object to our processing of their personal data for direct marketing purposes, or where we are relying on our legitimate interest (or those of a third party), where we cannot show a compelling reason to continue the processing.
- The right to request that we restrict our processing of their personal data. This enables individuals to ask us to suspend the processing of personal data about them, for example if they want us to establish its accuracy or the reason for processing it.
- The right to request that we transfer to them or another party, in a structured format, their personal data which they have provided to us (also known as the right to 'data portability'). The applicability of this right depends on the legal grounds on which we process it.
- The right to challenge a decision based solely on profiling/automated processing, to obtain human intervention, and to express their point of view.

We are required to comply with these rights without undue delay and, in respect of certain rights, within a one-month timeframe.

Individuals also have rights to complain to the local government body about, and to act in court to enforce their rights and seek compensation for damage suffered from, any breaches.

What you as an Employee need to do:

If you receive a request from an individual seeking to exercise a right in relation to their personal data or making an enquiry or complaint about our use of their personal data, you must forward the request, enquiry or complaint to your local Data Protection Representative immediately so that it can be dealt with appropriately and within the applicable time limit. Your assistance may be needed to address and respond to the request, enquiry or complaint.

Record keeping

In order to comply, and demonstrate our compliance, with data protection law, Studsvik keeps various records of our data processing activities. These include a Record of Processing which must contain, as a minimum: the purposes of processing; categories of data subjects and personal data; categories of recipients of disclosures of data; information about international data transfers; envisaged retention periods; general descriptions of security measures applied; and certain additional details for special category data.

What you as an Employee need to do:

You must also comply with our applicable processes / guidelines and any specific instructions you are given concerning the keeping of records about our processing of personal data.

If you are processing individuals' personal data in the course of your employment and you collect any new types of personal data or undertake any new types of processing activities, either through the introduction of new systems or technology or by amending existing ones, please inform your local Data Protection Representative so that we are able to keep our records up-to-date.

Training

We require all Employees to undergo basic training to enable them to comply with data protection law and this document. Additional training may be required for specific roles and activities involving the use of personal data.

To this end, we provide training as part of our introduction process for new joiners to Studsvik and operate an ongoing training program to make sure that Employees' knowledge and understanding of what is necessary for compliance in the context of their role is up-to-date. Attendance at such training is mandatory and will be recorded.

Departures from this document

There are some very limited exemptions from data protection law, which may permit departure from aspects of this Document in certain circumstances.

You will be given specific instructions if any exemptions are relevant to your role.

If you think you should be able to depart from this Document in any circumstances, you must contact your local Data Protection Representative before taking any action.

Studsvik AB
611 82 Nyköping
Sweden
+46 155 22 10 00

Studsvik