Duni AB (publ)

GDPR Policy and Instructions for the Duni Group

Approved by the Board of Directors on 12 July, 2018.
Approved by the Board of Directors on 11 July, 2019.
Approved by the Board of Directors on 14 July, 2020.

Duni AB • P.O. Box 237 • SE-201 22 Malmö • Sweden
Phone +46 40 10 62 00 • Telefax +46 40 39 66 30 • Visitors Ubåtshallen, Östra Varvsgatan 9a • Duni.com
Org.No. 5565367488 • Reg.Office Malmö

Comprehensive GDPR Policies and Instructions for the Duni Group

Summary of GDPR Principles

GDPR is the popular name for regulation (EU) 2016/679 and stands for General Data Protection Regulation. Its main purpose is to strengthen and unify data protection for all individuals within the European Union. It's interesting to note that GDPR is a **regulation** and not a directive. A regulation is applicable as it is written in all EU countries and there are no local differences. A directive is often interpreted and implemented differently in different EU countries. There, nevertheless, are many other laws which may be related to GDPR but not part of it which may differ greatly between countries. One example is for how long data needs to be archived. The UK is expected to adhere to GDPR even if Brexit is finalized.

*The main requirement of GDPR is that processing of personal data is only allowed if an organization has a **legitimate interest** in it. Only the personal data necessary to fulfil this legitimate interest is allowed. No extra, good-to-have data can be included. The data should also not be saved for longer than it is needed.*

One example is when a customer places an order. The organization has then the right to register the personal data necessary to complete the order. This would normally include name, address and e-mail but not hair colour, age and favourite football team and other non- essential information for the order. No special consent is needed from the customer for the organization to register this necessary data. The data registered in connection with the order is not allowed to be used for other purposes than fulfilling the order. If the organization would like to use the data for sending marketing material to the customer, then the customer must explicitly consent to this and the organization must be able to prove that consent was given.

When evaluating whether personal data can be processed or not you will normally come to a correct decision if you consider why it is needed and if only the necessary data will be processed. If the personal data is related to a transaction or normal, natural business relations, then it is OK to register without any special permission. Orders from customers and to suppliers are typical examples where some personal data processing normally is necessary. Other examples where personal data is needed are for employing people and interactions with counterparties such as potential clients, suppliers, government, banks and more. Please keep in mind that e-mails contain personal data and usually it is no problem to save these in connection with normal communication.

It is more difficult to answer the question about how long it is suitable or allowed to keep personal data. In the example of a customer order you can argue that the data should be saved for as long as accounting records need to be archived. There are, however, no clear guidelines about this.

Duni GDPR Compliance Policies

1. Employee Awareness

The most important element of GDPR compliance is the awareness and behaviour of employees or contractors within the organization. All employees shall complete a course in basic GDPR knowledge. This course shall be available and maintained in Duni's e-learning portal where it shall also be documented who has completed the course.

Training is obligatory for all new employees at the beginning of their employment. New employees shall conduct the e-learning course before or as soon as possible after the start of their employment. Contractors and temporary workers shall also take the course and this shall be documented in the same way as it is for regular employees.

The training package shall be available in local languages. It is, however, up to the employee to choose in which language they wish to complete the trainng.

Information about who has completed the GDPR course shall be deleted upon termination of employment or contract.

The GDPR course shall contain at least the following elements:

- General information about GDPR and the purpose of the regulation.
- That legitimate interest is the key element of GDPR compliance
- What is meant by structured and unstructured data and that GDPR is applicable to both.
- The basic requirements for an organization to be GDPR compliant.
- What is meant by sensitive personal data and how to process such data.
- The rights of data subjects
- When explicit consent is necessary from data subjects
- An explanation of what a Data Breach is and how to report it.

2. Documentation of Data Storage

Systems where structured personal data is stored shall be documented in a table and maintained. A person, normally a Data Administrator (see section

about this for definition), shall be appointed as responsible for maintenance of this table. Duni keeps this table on the GDPR SharePoint site. The table shall contain the following information:

- Name of System
- Responsible Legal Unit
- **Person Responsible** for Personal Data in the System
- Types of Personal Data Stored/ Processed
- Whether Sensitive Personal Data is Stored
- The Categories of Persons that are Registered
- To Whom Personal Data Stored/Processed in the System is Available
- In Which Countries the System is Used/ Available
- What Legitimate Interest Exists for Processing Personal Data in the System
- If the Personal Data is Needed to Fulfil a Legal Requirement
- If Consent from Data Subjects is Needed
- If Consent from Data Subjects is Documented
- How Personal Data is Collected and Registered in the System
- Additional Comments

Each person responsible for personal data of a system shall be contacted by a Data Administrator at least yearly to discuss compliance, changes and possible issues. This yearly contact shall be documented in Duni's GDPR checklist which is kept and updated on the GDPR SharePoint site.

3. Privacy by Design

Duni shall ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. Examples:

- building new IT systems for storing or accessing personal data
- developing policies or strategies that have privacy implications
- before engaging in a data sharing initiative
- using data for new purposes.

All existing processes, policies and IT systems shall be reviewed and adjusted so that adequate privacy and data protection is ensured.

Privacy Impact Assessments (PIAs) are tools that Duni should use to identify and reduce the privacy risks of projects and processes. With PIA methodology Duni can reduce the risks of harm to individuals through the misuse of their personal information. PIA:s can also help Duni to design more efficient and effective processes for handling personal data.

4. Sensitive Personal Data

Sensitive personal data is a specific set of “special categories” that must be treated with extra security. These categories are:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data

The general rule within Duni is that sensitive personal data shall not be processed. It is forbidden to e-mail, store in electronic or non-electronic form or in any way process sensitive data. If sensitive data is accidentally received, for example in an e-mail then it shall be deleted. If sensitive data is received in a CV related to an active recruitment process the person who sent it shall be informed and have the possibility to withdraw or replace the CV. See more about CV:s in the CV section of this guideline.

If sensitive personal data must be processed for legal or other reasons then special care shall be taken to protect the data from any unauthorized access and it shall be double checked whether it really is legitimate to process it. Please contact gdpr@duni.com in such cases.

5. Processing Unstructured Data

As is the case for all processing of personal data legitimate interest is also the key requirement for unstructured personal data. The most common forms of unstructured data are e-mails, documents and spreadsheets. If you have information containing names, e-mail addresses and other personal data this is acceptable if they are part of natural business activity. If you are in contact with suppliers concerning purchases, then you and the company certainly have a legitimate interest in processing this data. The same is true for customer contacts and all contacts with colleagues.

Most personal data obtained by Duni is in business-to-business relationships so it is normally not problematic. If you do process so called ‘true’ personal data of individuals, then you need to be careful. Such data could be private addresses, telephone numbers or personal information of any kind. An example of when such information could be obtained is when someone sends in a CV by e-mail or post. A CV and other private data needs to be treated with extra care. Do not save or spread such data unless you are confident that it is legitimate and controlled. If in doubt, contact gdpr@duni.com .

As stated in the section on sensitive personal data:

Sensitive personal data shall not be processed. It is forbidden to e-mail, store in electronic or non-electronic form or in any way process sensitive data. If sensitive data is accidentally received, for example in an e-mail then it shall be deleted.

Personnel who are in possession of or know about significant amounts of what is believed to be previously unknown unstructured personal data kept on Duni equipment or on Duni premises shall report this to gdpr@duni.com . It shall be reported why this data is processed and who is responsible for its maintenance including deletion.

6. Obtaining Consent

A common misconception about the GDPR is that all organisations need to seek consent to process personal data. In fact, consent is only one of six lawful grounds for processing personal data, and the strict rules regarding lawful consent requests make it generally the **least preferable option**.

The other lawful grounds are:

• A **contract** with the individual: for example, to supply goods or services they have requested, or to fulfil an obligation under an employee contract.
• Compliance with a **legal obligation**: when processing data for a particular purpose is a legal requirement.
• **Vital interests**: for example, when processing data will protect someone's physical integrity or life (either the data subject's or someone else's).
• A public task: for example, to complete official functions or tasks in the public interest. This will typically cover public authorities such as government departments, schools and other educational institutions; hospitals; and the police.
• **Legitimate interests**: when a private-sector organisation has a genuine and legitimate reason (**including commercial benefit**) to process personal data without consent, provided it is not outweighed by negative effects to the individual's rights and freedoms.

If none of the above five grounds are valid then explicit consent from the data subject is necessary. Examples of data processing when explicit consent is necessary is when data is processed primarily or purely for **marketing**

purposes. If you have a database with names and e-mail addresses and this is for sending a newsletter then explicit consent is necessary. If personal data has been obtained based on lawful ground, a contract for example, and then that data is to be used for something else, such as marketing, then explicit consent is also necessary.

If you are unsure about the necessity of explicit consent, then please contact Duni's Data Administrators by writing to gdpr@duni.com .

If explicit consent is necessary then certain requirements must be met. The consent request must be:

• **Unbundled**: ensure that consent requests are separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.
• **Granular**: give a thorough explanation of options to consent to different types of processing wherever appropriate.
• **Named**: state which organisation and third parties will be relying on consent – even precisely defined categories of third-party organisations will not be acceptable under the GDPR.
• **Documented**: keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented.
• **Easy to withdraw**: tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent. This means you will need to have simple and effective withdrawal mechanisms in place.
• **Without an imbalance** in the relationship: check that there isn't an imbalance in the relationship between the individual and the controller (such as an employee and employer, or a tenant and a housing association).

Consent given can at any time be revoked by the data subject. The company must communicate clearly to data subjects how they can revoke consent.

7. Website Privacy Policies

All Duni external websites must have a GDPR compliant privacy policy. Such a policy needs to inform about:

• What personally identifiable information is collected hrough the website, how it is used and with whom it may be shared.
• What choices are available to data subjects regarding the use of their data.
• The security procedures in place to protect the misuse of information.
• How any inaccuracies in the information can be corrected.

A privacy policy must also clearly inform about how the company can be contacted in case of any privacy issue. The standard contact for Duni is gdpr@duni.com .

8. Data Administrators

Duni shall have at least two Data Administrators for GDPR issues in each of Sweden, Germany and Poland. A Data Administrator shall be an employee and act as a contact and liaison internally and externally for personal data issues. A Data Administrator has no legal responsibility or special privileges like a Data Protection Officer. A Data Administrator needs good knowledge about GDPR but must not be an expert. The Data Administrators role is to take care of certain issues but also to forward some issues to colleagues and/ or experts for consultation or help.

A list of Data Administrators shall be kept on Duni's GDPR SharePoint site. Employees should contact Data Administrators by writing to gdpr@duni.com rather than directly to the personal e-mail address.

9. Data Protection Officers (DPO)

Duni shall **not** appoint a Data Protection Officer.

GDPR requires data controllers and processors to designate a DPO in any case where:

• the processing is carried out by a public authority or body
• the 'core activities' of the controller/processor consist of processing operations which 'require regular and systematic monitoring of data subjects on a large scale'
• the core activities of the controller/processor consist of processing on a large scale of 'special categories of data' or personal data relating to criminal convictions and offences

While the public sector is covered by the first requirement, the vast majority of private sector companies will not be required to appoint a DPO. Most private companies do not engage in systematic monitoring as a core activity and, to the extent that they process health, convictions or other sensitive/special categories of data, they do so in a manner that is incidental to their business, typically in the ordinary course of personnel administration.

Duni does not belong to a category of organizations required to appoint a DPO. The DPO role differs from most employees or contractors in that it is statutorily

independent and protected. DPOs must be independent, avoid conflicts of interest and they cannot receive instruction regarding the performance of their tasks. GDPR provides DPOs with protected employment status, meaning that organisations cannot dismiss or sanction DPOs for performing their tasks.

10. Reporting of Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Under the GDPR, breach notification will become mandatory in all member states where a data breach (=leak) is likely to "result in a risk for the rights and freedoms of individuals". This must be done within **72 hours** of first having become aware of the breach. If it takes longer than 72 hours to report a breach then an explanation for the delay must be added to the report.
When reporting a breach, the GDPR says you must provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

The GDPR recognises that it will not always be possible to investigate a breach

fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. You are, therefore, allowed to provide the required information in phases, as long as this is done without undue further delay.

All data notifications shall be sent to gdpr@duni.com . A Data Administrator will then evaluate the breach and take possible action such as reporting it to authorities.

11. Fulfilling Data Subject Rights

Private individuals have the following basic rights concerning data registered by an organization – the right to:

- to be informed
- to access
- correction
- deletion
- restrict processing
- to data portability
- to object
- voice special concerns about automated decision making and profiling.

The above rights (especially deletion) may be in conflict with laws or other legitimate interests an organization has for processing personal data. The rights are fully exercisable if the organization no longer has a valid need or legal requirement for processing the data.

There are two cases when you need to **proactively** inform about information processed:

1. When the personal data is collected from the individual it relates to. In such a case, they must be provided with privacy information at the time you obtain their data. This applies for personal data collected by a web site form, for example.

2. When you obtain personal data from a source other than the individual it relates to (for example if you purchase the info.), you need to provide the individual with privacy information:

- within a reasonable of period of obtaining the personal data and no later than one month;
- if the data is used to communicate with the individual, at the latest, when the first communication takes place; or
- if disclosure to someone else is envisaged, at the latest, when the

data is disclosed.

Personal data obtained in business-to-business transactions or discussions is normally not subject to these requirements unless the information is truly private and will be used for something else than the original intent. The same is true for necessary personal data collected from employees, contractors or colleagues.

A person who wishes to be informed about what data about them Duni processes need to file a subject access request (SAR) that is simply "an email, or letter asking for their personal data. If anyone in the organization receives such an e-mail or letter, then it should be forwarded to gdpr@duni.com . Upon receipt of such a request the legitimacy of the request should first be established. The person making the request shall be asked to identify himself in a trustworthy manner. Any information sent to the individual making the request shall be sent by post to the person's registered address or collected personally after showing valid identification. Duni may charge a "reasonable fee" when "a request is manifestly unfounded or excessive, particularly if it is repetitive."

Duni will not provide information about personal data which may be found in individual employee's e-mails or other files unless the person making such a request can provide a valid suspicion of wrongdoing, a police warrant or similar.

12. Data Processors

Whenever Duni employs a third party (Data Processor) to process personal data it needs to have a written contract in place – a Data Processing Agreement. Examples of such Data Processors are payroll providers and health care companies.

The contract is important so that both parties understand their responsibilities and liabilities.

According to GDPR the following needs to be included in the contract:

- the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
- the processor must ensure that people processing the data are subject to a duty of confidence;
- the processor must take appropriate measures to ensure the security of processing;

• the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
• the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
• the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
• the processor must delete or return all personal data to the controller as requested at the end of the contract; and
• the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Data Controllers (=Duni) are liable for their compliance with GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor which adheres to an approved code of conduct or certification scheme may help controllers to satisfy this requirement – though again, no such schemes are currently available.

Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

If a Data Processor is located outside the EES area (EU + Norway, Liechtenstein and Iceland), in a so-called third country, then that Data Processor must fulfil requirements for adequate protection. Examples of countries who according to the European Commission fulfil the requirements as of May 2018 are Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US. Each individual Third Country Data Processor should, however, be individually assessed.

Data Processing Agreements shall be reported to gdpr@duni.com and registered in a table by Data Administrators. It is recommended to consult with a Data Administrator before signing a Data Processing Agreement.

13. CV:s

CV:s shall be handled with care. Employees shall not forward CV:s by e-mail unless track is kept of whom it has been forwarded to and that the employee remembers to delete it from in- and outboxes and other locations after the

recruitment process is finished. If the CV has been forwarded, those who received it needs to be reminded to delete it. Ideally CV:s should be stored in a central location on the intranet or other application which allows access control and deletion. If the Company wants to keep a CV for longer than the recruitment process, it should ask for permission from the person whose data it concerns.

14. Photographs

Work-related photographs of employees and other people including portraits can be published and used internally on the intranet, internal files and similar. For all 'public' use of photographs containing identifiable persons, employees or others, consent is needed from the persons appearing on the pictures. Public use is for example publishing pictures or making them accessible on external websites, in catalogues or e-mailing to external parties.

15. Time Limits for Storing Personal Data

According to GDPR data should be stored for the shortest time possible. There are no guidelines to specify how long this is for different categories of data. There are some categories of data for which you can relatively easily establish how long it is appropriate to store the data. A CV should not be stored for longer than the recruitment process lasts and payroll data for as long as the law requires it (can be up to 50 years depending on country). More often it is completely up to the judgement of the organization processing the data. No guidelines will therefore be written into this document until more is known or possible guidelines published.

GDPR Checklist

The list shall be kept and updated Duni's GDPR SharePoint site. It shall contain at least the following:
