AVEGA

Société à responsabilité limitée

GDPR

(General Data Protection Regulation)

Content

1. Background

The EU General Data Protection Regulation (GDPR) is designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the countries approach data privacy.

The GDPR applies to all EU organisations – whether commercial business, charity or public authority – that collect, store or process the personal data of individuals residing in the EU, even if they are not EU citizens. Organisations based outside the EU that offer goods or services to EU residents, monitor their behaviour or process their personal data will be subject to the GDPR. Service providers (data processors[1]) that process data on behalf of an organisation come under the remit of the GDPR and will have specific compliance obligations.

Avega Group[2] has issued this policy which is addressed to individuals outside our organisation with whom we interact.

Avega Group has established a culture of monitoring, reviewing and assessing data processing procedures, minimizes data processing and retention of data and has built up safeguards to data processing activities.

Avega Group has reviewed all aspects of personal data processing and is implementing plans designed to ensure compliance with the requirements of GDPR.

2. Personal Data

Personal data is any information relating to an identified or identifiable private individual, whether it relates to his or her private, professional or public life. An identifiable individual is one who can be identified either directly or indirectly, for example, through the use of an identifier, such as an identification number. Personal data therefore covers a vast amount of information and can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking

[1] The data processor processes personal data only on behalf of the controller. The data processor is usually a third party external to the company.
[2] Avega Group: Avega S.à r.l., Avega Revision S.à r.l., Avega Tax Advisors S.à r.l., Avega Services (Luxembourg) S.à r.l., Avega Netherlands B.V., Avega Fund Services S.à r.l., Avega Capital Management S.A., Avega Spain Corporate Services S.L. and Avega France SAS.

websites, medical information or a computer's IP address. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Specific examples include but are not limited to:

- ID card
- Image of ID document
- KYC identifiers
- Domicile address
- Secondary residence address
- Postal address (may differ from domicile or secondary residence addresses)
- Nationality (sometimes double nationality, etc.)
- Marital status
- Gender
- Profession information: job title, cadre level, fiscal (tax) status
- Business cards
- Account number
- Email addresses
- Pseudonyms
- Internet Protocol (IP) address;

All personal data, including pseudonymous data, regardless of the format or physical storage, must be protected. The obligation to protect personal data applies both to static as well as transactional data.

3. Data processing

Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

The General Data Protection Regulation (GDPR) applies to the processing of personal data wholly or partly by automated means as well as to non-automated processing, if it is part of a structured filing system.

Collection of personal data about individuals is done via the following sources:

- The individual provides the personal data directly to Avega Group via email, telephone etc.
- Avega Group receives the personal data in the ordinary course of the relationship with the individual (e.g. administration of the companies)
- Avega Group receives the personal data from third parties (e.g. lawyers)

The type and amount of personal data Avega Group may process depends on the reason for processing it and the intended use. Avega Group respects several key rules, including:

- personal data are processed in a lawful and transparent manner, ensuring fairness towards the individuals whose personal data is being processed ('lawfulness, fairness and transparency');
- there must be a specific purpose for processing the data and Avega Group indicates that purpose to individuals when collecting their personal data. Avega Group does not simply collect personal data for undefined purposes ('purpose limitation');
- Avega Group collects and processes only the personal data that is necessary to fulfil that purpose ('data minimisation');
- Avega Group ensures that the personal data is accurate and up-to-date, having regard to the purposes for which it is processed, and correct it if not ('accuracy');
- Avega Group does not use the personal data for other purposes that aren't compatible with the original purpose;
- Avega Group ensures that personal data is stored for no longer than necessary for the purposes for which it was collected ('storage limitation');
- Avega Group has installed appropriate technical and organizational safeguards that ensure the security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technology ('integrity and confidentiality').

Personal data should only be processed where it is not reasonably feasible to carry out the processing in another manner. Where possible, it is preferable to use anonymous data. Where personal data is needed, it should be adequate, relevant, and limited to what is necessary for the purpose (‘**data minimisation’**). It is Avega Group's responsibility as controller to assess how much data is needed and ensure that irrelevant data is not collected.

4. When can personal data be processed?

Avega Group will only process personal data in the following circumstances:

- with the consent[3] of the individuals concerned;
- to meet a legal obligation under EU or national legislation;
- where processing is necessary for the performance of a task carried out in the public interest under EU or national legislation;
- fairly and lawfully
- to fulfill a contractual obligation (a contract between Avega Group and a client);
- for the organization’s legitimate interests, but only after having checked that the fundamental rights and freedoms of the person whose data are being processed are not seriously impacted. If the person’s rights override the interests, then processing cannot be carried out based on legitimate interest. The assessment as to whether Avega Group has a legitimate interest for processing to override those of the persons concerned depends on the individual circumstances of the case.

[3] „consent“ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject`s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data to him or her

5. What information must be given to individuals whose data is collected?

At the time of collecting personal data, Avega Group will inform clearly about at least:

- who the company/organization is (contact details);
- why the company/organization will be using personal data (purposes);
- the categories of personal data concerned;
- the legal justification for processing the data;
- for how long the data will be kept;
- who else might receive it;
- whether the personal data will be transferred to a recipient outside the EU;
- that the individuals have a right to receive a copy of the data (right to access personal data) and other basic rights in the field of data protection (see complete list of rights; Art. 13 GDPR);
- right to lodge a complaint with a Data Protection Authority (DPA);
- right to withdraw consent at any time;
- where applicable, the existence of automated decision-making and the logic involved, including the consequences thereof.

6. 'by design' / 'by default'

Avega Group has implemented technical and organizational measures, at the earliest stages of the design of the processing operations, in such a way that safeguards privacy and data protection principles right from the start ('data protection **by design'**).

Avega Group has ensured that personal data is processed with the highest privacy protection (for example only the data necessary should be processed, short storage period, limited accessibility) so that by default personal data is not made accessible to an indefinite number of persons ('data protection **by default'**).

7. Data subjects' rights

These include, for example, a right to require information about data being processed about the individual, access to the data in certain circumstances, and correction of data which is wrong. Individuals can also ask Avega Group to receive their personal data in a structured and commonly used format so that it can easily be transferred to another data controller[4] ("**data portability**"). The "**right to be forgotten**" or "**right of erasure**" allows individuals to require Avega Group to erase their personal data without undue delay in certain situations, such as where they withdraw consent and no other legal ground for processing applies. The information shall be provided free of charge by Avega Group unless the request is manifestly unfounded or excessive.

7.1. Right of Access (Also known as a Subject Access Request):

Data Subjects have the Right to obtain:

- Confirmation that their data is being processed
- Access to their personal data and
- Other supplementary information

Right of access requests must be responded to within one month.

7.2. Right to Rectification:

Data Subjects are entitled to have their personal data rectified if it is inaccurate or incomplete. If the information in question has been disclosed to a third party the Data Controller must inform them of the request for rectification where possible. The Data Subject is also entitled to be informed of the third parties to whom the data has been disclosed, where appropriate.

[4] The data controller determines the purposes for which and the means by which personal data is processed.

Rights to rectification must be responded to within one month.

7.3.Right to Erasure:

This Right is also known as the ‘Right to be Forgotten’. It enables Data Subjects to request the deletion or removal of personal data where there is no compelling reason for its continued processing by the Data Controller.

The Right to Erasure applies in the following circumstances:

- The personal data is no longer necessary in relation to the purpose for which it was originally collected
- The processing was based on consent, and the Data Subject has now withdrawn their consent
- The Data Subject objects to processing and there is no overriding legitimate interest of the Data Controller
- The data was being unlawfully processed
- The data must be erased to comply with a legal obligation

7.4.Right to Restrict Processing:

When this Right is exercised you are permitted to store the personal data but not further process it. Restricted information about the individual may be retained to ensure that the restriction is respected in the future.

The Right to Restrict Processing applies in the following circumstances:

- When a Data Subject contests the accuracy of their personal data, then processing should be restricted to storage only until accuracy is verified
- When a Data Subject objects to processing which is being carried out for the reason of performance of a task in the public interest, or for the legitimate interests of the Data Controller, then the Data Controller must restrict processing to storage only whilst they consider whether their legitimate grounds override the Rights and freedoms of the individual.
- When processing is unlawful and a Data Subject opposes erasure and requests restriction
  instead.
- When the Data Controller no longer needs the personal data but the Data Subject requires it for the purpose of a legal claim.

7.5.Right to Data Portability:

This Right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows the individual to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way in a common data format, for example, Excel or CSV file.

The Right to Data Portability applies in the following circumstances:

- When the personal data was provided to the controller directly by the Data Subject
- Where the processing is based on consent or performance of a contract
- When processing is carried out by automated means

7.6.Right to Object:

Individuals have the Right to object to:

- Processing based on legitimate interest or performance of a task in the public interest/exercise of official authority (including profiling)
- Direct marketing (including profiling)
- Processing for the purposes of scientific/historical research and statistics

7.7.Rights in Relation to Automatic Decision Making and Profiling:

This Right provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

The Right not to be subject to a decision applies when:

- It is based on automated processing
- It produces legal/significant effects on the individual

It does not apply if the decision:

- Is necessary for entering into or performance of a contract
- Is authorised by law
- Is based on explicit consent
- Does not have a legal/significant effect on the data subject

8. Disclosure of Personal Data to third parties

We may disclose personal data to other entities within Avega Group, for legitimate business purposes in accordance with applicable law. In addition, we may disclose personal data to:

- Governmental, legal regulatory, or similar authorities, ombudsmen, and central and/or local government agencies, upon request or where required, including for the purposes of reporting any actual or suspected breach of applicable law or regulation;
- Accountants, auditors, financial advisors, notary, lawyers and other outside professional advisors, subject to binding contractual obligations of confidentiality;
- Third party processors (such as payment services providers, etc.) located anywhere in the world, subject to the requirements noted below in this section;
- Any relevant party for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security in accordance with applicable law

If we engage a third party processor to process the personal data, Avega has to ensure that the processor will be subject to binding contractual obligations to:

- Only process the personal data in accordance with Avega's prior written instructions and
- Use measures to protect the confidentiality and security of the personal data; together with any additional requirements under applicable law.

9. International transfers of personal data

EU data protection rules apply to the European Economic Area (EEA), which includes all EU countries and non-EU countries Iceland, Liechtenstein and Norway. When personal data is transferred outside the European Economic Area, special safeguards are foreseen to ensure that the protection travels with the data. Personal data can only

be transferred to a third country if that third country ensures an ‘adequate level of protection’ of personal data.

Data may also be transferred to third countries whose data protection level is deemed sufficient by the European Commission. The Commission has so far recognized Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand and Uruguay as providing "adequate" protection.

The controller has to examine the level of protection of personal data in the relevant third country before transferring the data. There is no exception for a transfer of personal data between entities within the same group.

Where the personal data is transferred to other countries outside EU and Iceland, Liechtenstein and Norway, this is done on the basis of standard contractual clauses and explicit approval of the affected person.

10. Data breach

Avega Group has to notify the supervisory authority without undue delay and at the latest within **72 hours** after having become aware of the breach. If Avega Group is a data processor, it must notify every data breach to the data controller. Breach by processor has to be reported within 72 to Avega Group.

11. Contact details

data.protection@avega.lu
2, rue Edward Steichen,
L-2540 Luxembourg
Phone: +352 246 943-1; Fax: +352 246 943-70