Data Protection Guideline of Verallia Deutschland AG

Table of Contents

1. Aims of the data protection guideline

Verallia Deutschland AG, as part of its social responsibility obligations, undertakes to comply with European and international measures to maintain data protection rights according to the new EU General Data Protection Regulation. This data protection guideline applies world-wide for Verallia Deutschland AG and is based on globally accepted basic principles of data protection.

As a result, data protection and data security are, with regard to modern information and communication technologies and the growing commercial value of personal data, vital cornerstones of the information society. Good reasons for modern data protection are on the one hand the protection of every individual's privacy in the information age. On the other hand, data protection in modern commercial life is a quality factor, becoming ever more important in the course of globalisation. Maintaining data protection forms a base for business relationships founded on trust and the reputation of Verallia Deutschland AG as an attractive employer.

2. Scope and amendments to the data protection guideline

This data protection guideline is based on the provisions of the EU General Data Protection Regulation and the accompanying national laws.

This data protection guideline applies to the whole of Verallia Deutschland AG in all its locations.

3. Principles for processing personal data

3.1 Fairness and lawfulness

When processing personal data, the right of the data subject to informational self-determination must be assured. Personal data must be collected and processed lawfully.

3.2 Purpose

Processing of personal data may only be for purposes that have been determined before the data was collected. Subsequent changes to the purposes can only be made to a limited extent and require justification.

3.3 Transparency

The data subject must be informed about the manner in which his or her data are handled. In principle, personal data should be recorded by the data subjects themselves. When the data are collected, the data subject must be able at least to recognise the following or be informed accordingly:

- The identity of the party responsible
- The purpose of data processing
- The stored retention periods
- Third parties or categories of third parties to whom the data may be transferred

The duty of information exists for interested parties, customers and employees.

3.4 Data avoidance and data economy

Before any processing of personal data, checks should be made as to whether and to what extent these data are required to achieve the purpose intended by processing. If it is possible for achieving the purpose and the expenditure is reasonable for the intended purpose, anonymised or statistical data should be used. Personal data may not be kept stored for potential future purposes, unless this is prescribed or permitted by national legislation.

3.5 Deletion and limitation of storage time

Personal data that are no longer required once legal or business transaction-related storage periods have expired must be deleted. If in individual cases there are indications of interests warranting protection or of historic importance of these data, the data must continue to be stored until the interests warranting protection have been legally clarified.

3.6 Factual accuracy and data currency

Personal data must be saved correctly, completely and – insofar as this is possible – in their current version. Suitable measures must be taken to ensure that incorrect, incomplete or outdated data are deleted, corrected, completed or updated.

3.7 Confidentiality and data security

Data secrecy applies to personal data.

They must when personally handled be treated as confidential and secured by appropriate organisational and technical measures against unauthorised access, wrongful processing or disclosure, as well as accidental loss, alteration or destruction.

3.8 Admissibility of data processing

The collection, processing and use of personal data is admissible only if one of the following permissions exists. Such permission is also required if the purpose of the collection, processing and use of the personal data is to be changed from the originally determined purpose.

4. Customer and partner data

4.1 Data processing for a contractual relationship

If the processing of personal data serves the performance of a contract or the fulfillment of pre-contractual measures, the processing is admissible.

4.2 Consent to data processing

Data processing may be carried out based on consent by the data subject. Before consenting, the data subject must be informed in accordance with this data protection guideline. For reasons of evidence, the declaration of consent must be obtained in writing or electronically. In certain circumstances, e.g. with consultation by telephone, consent can also be given orally. Consent must be documented.

4.3 Data processing based on legal permission

Processing of personal data is also admissible if national legal provisions demand, require or permit it. The type and scope of the data processing must be that required for legally admissible data processing and will conform with these legal provisions.

4.4 Data processing based on legitimate interest

The processing of personal data can also be carried out if this is required to realise a legitimate interest of Verallia Deutschland AG. As a rule, legitimate interests are of a legal (e.g. calling in outstanding receivables) or economic (e.g. avoiding disruption to contracts) nature. Processing of personal data based on legitimate interest may not take place if in an individual case there is an indication that the data subject's interests warranting protection take precedence. The interests warranting protection must be checked for every instance of processing.

4.5 Processing of data requiring special protection

The processing of personal data requiring special protection may only be carried out if this is legally required or the data subject has given explicit consent. The processing of these data is also admissible if it is essential for making, exercising or defending legal claims against the data subject.

4.6 Automatic individual decisions

Automatic processing of personal data used to evaluate individual personal characteristics (e.g. credit-worthiness) may not be the sole foundation for decisions with negative legal consequences or considerable negative effects on the data subject. The data subject must be notified of the fact and of the result of an automatic individual decision and given the option to comment upon it. To avoid mistaken decisions, checks and a plausibility test must be made by an employee.

4.7 User data and the internet

If personal data are collected, processed and used from websites or in apps, the data subjects must be informed of this in data protection declarations or if required in references made to cookies. The references made to data protection and if required to cookies must be integrated in such a way as to be easily recognisable, directly accessible and constantly available to the data subject.

If user profiles are created to evaluate user behaviour with websites and apps (tracking), the data subjects must be informed of this in every case in the data protection declarations. If the tracking is carried out using a pseudonym, the data subject should have an option to object in the data protection declarations (opt-out).

5. Employee data

5.1 Data processing for the employment relationship

Personal data that is relevant for the foundation, implementation and termination of the contract of employment may be processed for the working relationship.

At the approach to a working relationship, personal data of applicants may be processed. If the applicants are rejected, their data are to be deleted in accordance with the obligations of limits for the rules of evidence, unless the applicant has consented to further storage for a subsequent selection process. Consent is also required for the use of the data for further application procedures or before the application is passed on to other parts of the company.

Data processing in the existing work relationship must always be with reference to the purpose of the contract of employment, unless one of the following permissions for data processing takes effect.

If during the approach to the working relationship or in the existing working relationship it is necessary to collect further information about the applicant from a third party, the relevant national legal requirements must be taken into account. In case of doubt, the consent of the data subject must be obtained.

There must be legal legitimacy in every case of processing of personal data that are within the context of the working relationship but do not inherently serve the performance of the contract of employment. These could be legal requirements, collective agreements with employer representatives, the consent of the employee or the legitimate interests of the company.

5.2 Data processing based on legal permission

The processing of employees' personal data is also admissible if national legal provisions demand, require or permit it. The type and scope of the data processing must be that required for legally admissible data processing and conform with these legal provisions. If there is any legal room for manoeuvre, the legitimate interests of the employee must be taken into account.

5.3 Collective regulations for data processing

If an instance of processing exceeds the purpose of contract implementation, it is admissible if permitted by a collective regulation. Collective regulations are tariff agreements or agreements between employees' and employers' representatives within the framework of possibilities of the relevant employment law. These regulations must cover the specific purpose of the intended processing and can be devised within the framework of national data protection law.

5.4 Consent to data processing

Processing of employee data may be carried out based on consent by the data subject.

Declarations of consent must be made voluntarily. Non-voluntary consent is invalid. For reasons of evidence, the declaration of consent must be obtained in writing or electronically. If in exceptional cases the circumstances do not allow this, consent can be given orally. In every case, the giving of consent must be documented properly. If there is an informed, voluntary submission of data by the data subject, consent may be assumed if national law does not prescribe explicit consent. Before consenting, the data subject must be informed in accordance with this data protection guideline.

5.5 Data processing based on legitimate interest

The processing of employees' personal data can also be carried out if this is required to realise a legitimate interest of Verallia Deutschland AG. Legitimate interests are as a rule legally (e.g. the making, exercising or defence of legal claims) or economically based.

Processing of personal data based on a legitimate interest may not be carried out if in an individual case there is an indication that the employee's interests warranting protection outweigh the interest in processing. The existence of interests warranting protection must be checked for every instance of processing.

Control measures that require the processing of employee data may only be carried out if there is a legal obligation to do so or or reasonable grounds exist. Even if reasonable grounds exist, the proportional nature of the control measure must be checked. The legitimate interests of the company in carrying out the control measure (e.g. compliance with legal provisions and internal company rules) must be weighed against any possible interest warranting protection of the employee affected by it in the exclusion of the measure; measures may only be carried out if they are proportionate. The legitimate interests of the company and the interests warranting protection of the employees must be determined and documented before every measure. In addition, further requirements, possibly in accordance with national law (e.g. co-determination rights of the employees' representatives and information rights of the data subjects), must be taken into account.

5.6 Processing of data requiring special protection

Personal data requiring special protection may only be processed under certain conditions. Personal data requiring special protection are data concerning racial and ethnic origin, political opinions, religious or philosophical convictions, trade union membership or the health or sexuality of the data subject.

Equally, data concerning criminal offences may also often only be processed under special conditions set by national law.

Processing must be explicitly permitted or prescribed based on national law. In addition, processing may be permitted if it is necessary for the department responsible to comply with its rights and duties in the field of employment law. The employee may also voluntarily give explicit consent to the processing.

5.7 Automatic decisions

Insofar as personal data which are used to evaluate individual characteristics (e.g. as part of personnel selection or to evaluate skills profiles) are automatically processed within the employment relationship, such automatic processing may not be the sole foundation for decisions with negative consequences or considerable negative effects on the data subjects among the employees.

In order to avoid wrong decisions, the automatic processing must ensure that the facts it contains are assessed by a natural person and that this assessment forms the foundation for the decision. The data subject must also be notified of the fact and the result of the automatic individual decision and be given the option to comment upon it.

5.8 Telecommunications and the internet

Telephone systems, e-mail addresses, intranet and internet and internal social networks are primarily made available by the company for use in carrying out operational tasks. They are work equipment and company resources. They may be used within the framework of relevant applicable legal provisions and the internal company guidelines.

General monitoring of telephone and e-mail communication and of intranet and internet use will take place. To defend against attacks on the IT infrastructure or individual users, protective measures have been implemented at the transition points to Verallia that will block technically damaging content or analyse the pattern of attacks. For reasons of security and traceability, the use of telephone systems, e-mail addresses, intranet and internet, as well as internal social media, is logged. Personal assessments of these data may only be carried out if there is a specific well-founded suspicion of a breach of law or of the guidelines of Verallia Deutschland AG. These controls may only be carried out in compliance with the principle of proportionality. The relevant national laws must be observed, as must the internal group regulations that apply in this matter. These assessments cannot be used to record performance.

6. Transfer of personal data

Any transfer of personal data to recipients either outside Verallia Deutschland AG or within Verallia Deutschland AG is subject to the provisions of admissibility for processing personal data. The recipient of the data must be obliged to use these only for predetermined purposes.

In the event of a data transfer to a recipient outside Verallia Deutschland AG in a third country, that country must be able to guarantee a standard of data protection equivalent to this data protection guideline. This does not apply if the transfer is made because of a legal obligation.

In the event of a data transfer by third parties to Verallia Deutschland AG, there must be assurance that the data can be used for the purposes intended.

7. Contract data processing

Contract data processing takes place if a contractor is tasked with the preparation of personal data without having been given responsibility for the accompanying business transaction. In these cases, a contract data processing agreement must be concluded with external contractors.

The commissioning company retains full responsibility for the correct execution of the data processing. The contractor may only process personal data within the limits of the instructions given by the principal. When the contract is awarded, the following provisions must be complied with; the specialist department commissioned must ensure their implementation.

a) The contractor is to be selected according to its ability to guarantee the required technical and organisational protective measures.

b) The contract must be issued in text form. The instructions for data processing and the responsibilities of the principal and the contractor are to be documented.

c) Before data processing begins, the principal must assure itself that the contractor will comply with its duties. A contractor may, in particular, demonstrate compliance with the requirements of data security by submitting suitable certification. According to the risk of the data processing, monitoring may be regularly repeated in the course of the duration of the contract.

d) In the case of cross-border contract processing, the relevant national requirements for the disclosure of personal of data abroad must be met. In particular, processing of personal data from the European Economic Area may only take place in a third country if the contractor can demonstrate a standard of data protection equivalent to this data protection guideline.

e) Recognition of the contractor's binding company regulations to create an appropriate data protection standard shall be via the data protection authorities responsible.

8. Rights of data subjects

Every data subject may exercise the following rights. Claims according to these rights must be processed by the responsible department immediately and may not lead to any detrimental consequences for the person affected.

a) The data subject can demand information as to which of his or her personal data from which point of origin are stored for what purpose. If within the working relationship according to the relevant employment law further rights to inspect the employer's documentation are provided (e.g. personal file), these shall remain unaffected.

b) If personal data are transferred to third parties, information must also be provided on the identity of the recipient or on the categories of recipients.

c) If personal data should prove to be incorrect or incomplete, the data subject can demand that they be corrected or completed.

d) The data subject can object to the processing of his or her personal data for purposes of advertising or market and opinion research. The data must be blocked for these purposes.

e) The data subject is entitled to demand deletion of his or her data if the legal foundation for the processing of the data is missing or has ceased. The same applies to a case where the purpose of the data processing has ceased due to the expiry of time or for other reasons. Existing duties of storage and the deletion of opposing interests warranting protection must be observed.

f) The data subject has a fundamental right of objection to the processing of his or her data that must be taken into account if his or her interests warranting protection, based on a personal situation, outweigh the interests in processing. This does not apply if there is a duty to process the data due to a legal provision.

9. Confidentiality of processing

Personal data are subject to data secrecy. Employees are prohibited from unauthorised collection, processing or use.

Unauthorised processing is any processing an employee undertakes without having been entrusted with it as part of the performance of his or her tasks and without corresponding authorisation. The need-to-know principle applies: employees may only obtain access to personal data if and insofar as it is required for their relevant tasks. This requires the careful allocation and separation of roles and responsibilities together with their implementation and maintenance within the framework of authorisation concepts.

Employees may not make use of personal data for their own private or economic ends, transfer these to unauthorised or make them accessible in some other way.

10. Processing security

Personal data must be protected at all times against unauthorised access, improper processing or disclosure, as well as against loss, falsification or destruction. This applies regardless of whether it is carried out electronically or in paper form. Before the introduction of new data processing procedures, in particular new IT systems, technical and organisational measures to protect personal data are to be determined and implemented. These measures must be oriented towards the status of technology, the risks arising from processing and the need for protection of the data (to be determined by the process of information classification).

The technical and organisational measures to protect personal data form part of the company-wide information security and data management and must be continuously adapted to reflect technical developments and organisational changes.

11. Data protection monitoring

Compliance with the guidelines on data protection and the applicable data protection law will be regularly checked by data protection audits and further monitoring.

Company management is to be informed of the results of data monitoring.

12. Data protection incidents

Every employee should immediately report any infringements of this data protection guideline or other provisions for protecting personal data (data protection incidents) to the management.

In cases of

- ➜ improper transfer of personal data to third parties,
- ➜ improper access by third parties to personal data, or
- ➜ the loss of personal data

the notification options provided within the company (Information Security Incident Management) must be made use of immediately, so that the national legal reporting duties for data protection incidents can be complied with.

13. Responsibilities and sanctions

The management is responsible for conforming to the Regulation in the processing of personal data.

This means it has a duty to ensure that legal data processing requirements and requirements contained in the data processing guideline are met (e.g. national reporting duties).

It is the task of the company management to make use of organisational, personnel and technical measures to ensure proper data processing taking data protection into account. The competent employees are responsible for the implementation of these provisions. In the event of data protection monitoring by official bodies, the data protection officer must be informed immediately.

The management boards are to be named to the data protection officer.

The data protection officer is the on-site contact for data protection. He or she can carry out monitoring checks and is to familiarise the employees with the content of the data protection guidelines. The management has a duty to support the data protection officer in his or her activities. Those professionally responsible for the business processes and projects must inform the data protection officer in good time of new processing of personal data. With data protection projects that could result in particular risks for the personal data of the data subjects, the

data protection officer must be involved even before the start of data processing. This applies in particular to personal data requiring special protection.

The management must ensure that its employees are trained to the required extent in data protection. An improper processing of personal data or other breaches of data protection law are also prosecuted in many countries and can incur claims for compensation. Infringements for which individual employees are responsible can lead to sanctions under employment law.

14. The data protection officer

The data protection officer works as an internal body independent of professional instruction to maintain the provisions of data protection.

He or she is responsible for the monitoring of compliance with the data protection guidelines.

The data protection office will instruct the management promptly on data protection risks.

Every data subject may approach the data protection officer with suggestions, inquiries, requests for information or complaints in connection with data protection or data security. If requested, inquiries and complaints will be treated confidentially.

15. Implementation

This document will be checked once a year and when required for completeness and currency.

Amendments to this document are the responsibility of the person responsible for data protection management.

This document is to be kept accessible for all employees.