Privacy Policy & GDPR Guidelines

Assured Technologies SAS

Version 1.3

25.07.2025

Table of contents

PREAMBLE

Assured Technologies SAS takes the protection of personal data of employees, contractual partners, customers, suppliers and interested parties very seriously. For us, safeguarding and protecting the personal rights and privacy of each individual is the basis for trusting and successful business relationships. In order to ensure this protection and to illustrate the great importance of safeguarding personal rights and privacy, we have decided to issue this internal data protection policy.

In this policy, we have regulated the conditions for the processing of personal data of customers, suppliers, interested parties, business partners and employees. In accordance with European data protection legislation, we have defined seven principles for the processing of personal data in order to ensure a uniformly high level of data protection in our company. All managers, employees, employees, etc. are obliged to comply with this data protection policy as well as the applicable European and German data protection laws. The data protection policy is intended to be a guideline for all employees on how the handling of personal data is legally permissible and permitted in our company and is intended to answer the most important questions in data protection.

I. SCOPE

1. Personal Scope

This Privacy Policy applies to all employees of Assured Technologies SAS. For the purposes of this Directive, "employees" in this sense include not only full-time and part-time employees, as well as employees and trainees for their vocational training, but also all temporary agency workers and employees of external companies who work in the company.

2. Territorial scope

This policy applies to all employees at the company's locations and headquarters, as well as to all employees outside the company's headquarters (sales representatives, employees working from home, seconded employees, etc.).

3. Material scope

The rules, commandments and prohibitions of this policy apply to all handling of personal data, whether electronic or paper. In addition, they include all types of affected parties (employees, customers, suppliers, interested parties, etc.) in their scope.

4. Commitment to confidentiality and data secrecy

All employees and employees of Assured Technologies SAS are obliged to maintain confidentiality and to comply with the data protection requirements of the GDPR (hereinafter referred to as the "Declaration of Commitment") in accordance with the requirements of the GDPR or the applicable data protection laws. In the case of new hires, this declaration of commitment must be submitted together with the employment contract and signed by the future employee. The Declaration of Commitment is available from the Human Resources Department and may not be changed unless the Human Resources Department approves a change in writing after consultation with the Data Protection Officer.

II. ESSENTIAL TERMS OF DATA PROTECTION

1. Personal data

For the purposes of this Directive, the term "personal data" corresponds to the term "personal data" under the GDPR and the BDSG (new). Personal data means any information relating to an **identified** or **identifiable natural person** . An identifiable natural person is one who is directly or indirectly, for example by reference to an identifier such as a name, an identification number, location data, an online

identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2. Processing of personal data

Processing means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination: restriction, deletion or destruction.

3. Person in charge

The controller is any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

4. Processor

Processor means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

III. GENERAL PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA AND DATA SECURITY

1. Lawfulness of processing, fairness

Personal data may only be processed lawfully, fairly and in a manner that is comprehensible to the data subject. The personal rights of the person concerned must be respected.

2. Transparency

The data subject must be informed about the processing of his or her personal data. The data subject must be given the opportunity to exercise his or her so-called rights as a data subject and his or her right to informational self-determination. In principle, personal data must be collected from the data subject himself/herself. When personal data is collected, the data subject must be informed of the identity of the controller, the purposes of the processing, third parties/categories of third parties to whom the data may be transferred, and any other information that ensures fair and transparent processing of personal data. For the purpose of documentation, such information must be provided in writing.

The information and communications on the processing of personal data must be easily accessible and comprehensible and written in clear and simple language. In addition, the data subject must be confirmed or provided with information as to whether and which of the personal data in question is being processed (more on this under points XIII, XIII. Rights of data subjects). If you obtain personal data of this person from a third party - without the knowledge of the data subject or without his or her cooperation - care must be taken to ensure that this data subject is fully informed about the handling of his or her data at the time determined by law in Art. 14 GDPR, if he or she has not already been informed or if the law permits a waiver of the information. The requirements of Art. 14 GDPR must be complied with in order to ensure fair and transparent processing.

3. Earmarking

Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner incompatible with those purposes. A change of purpose is only permissible in exceptional cases and if there is a separate legal basis for it.

4. Data minimization

Personal data may only be processed in a manner appropriate to the purpose and limited to what is necessary for the purposes of the processing.

5. Correctness

Personal data must be accurate and, where necessary, up-to-date. All reasonable measures must be taken to ensure that personal data that are inaccurate in relation to the purposes for which they are processed are erased or rectified without undue delay.

6. Storage Limitation and Deletion

Personal data may only be stored in a form that allows the identification of the data subjects only for as long as is necessary for the purposes for which they are processed. If personal data is no longer required after the expiry of statutory or business process-related retention periods, it must be deleted in accordance with the standard.

7. Integrity and confidentiality

In addition, personal data may only be processed in a manner that ensures adequate security of the personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by means of appropriate technical and organisational measures.

8. Prohibition subject to authorisation

In data protection, a so-called prohibition with reservation of permission applies. It follows that, in principle, all data-relevant measures, any processing of personal data, are unlawful, unless a legally standardised reason for permission, a law or the consent of the data subject justifies or permits the measures or processing.

9. Restricting the use of IT

The use of IT systems and applications in the company is only permitted for business purposes and to the extent permitted in each case for the completion of tasks. The installation of software for private purposes is strictly prohibited.

In addition, only software that has been approved by the employer or the IT department may be installed on the company's IT systems. The approval is sent in writing, by e-mail to the Head of IT. After consultation with the management, this will be upheld or not granted. If new software is to be installed at the request of a specialist department, an investment application must first be submitted and the IT department must be fully informed about the desired software so that it can arrange for a data protection impact assessment to be carried out if necessary (for more details on the data protection impact assessment, see points VIII, VIII DATA PROTECTION IMPACT ASSESSMENT).

The use of private hardware and software for business purposes is not permitted, i.e. the processing of personal data on or with private hardware or software is prohibited.

10. Design of the workplace

The workplace must be designed by each employee in such a way that visitors or other third parties cannot gain access to personal data without being authorised to do so. For example, offices must always be locked after leaving the workplace, and documents must be locked away. When leaving the workplace PC, the respective employee must "log out", so that authentication (user name/password) is required before using the IT system and/or application(s) again. In areas with public traffic, the IT systems – in particular the screens – must be designed in such a way as to exclude the risk of being noticed by visitors or third parties as far as possible.

Information in paper form must be stored in such a way that visitors or other third parties cannot gain knowledge of the data. Confidential information must be kept under lock and key at all times.

IV. LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

The processing of personal data is generally prohibited unless a legal regulation expressly permits the handling of data. This means that data processing by employees of Assured Technologies SAS is only permissible if the following principles and one of the permitted circumstances for the processing of personal data of customers, suppliers, partners, interested parties or personal data of employees (employees, trainees, temporary workers, etc.) is met.

1. Principles for the processing of personal data

1.1 Earmarking

Personal data of customers, suppliers, partners, interested parties or personal data of employees shall only be processed for a pre-determined, explicit and legitimate purpose communicated to the data subject. Data storage without a purpose, e.g. the storage of data for retention, is not permitted.

In addition to the declared consent of the respective data subject, the change of the purpose and purpose of the data handling is only permissible if the purpose of the further processing is compatible with the original purpose. In particular, the reasonable expectations of the data subject vis-à-vis the company with regard to such further processing, the type of data used, the consequences for the data subject and the possibilities of encryption or pseudonymisation must be taken into account.

1.2 Data minimization

If possible, personal data should not be handled. The fact that, for example, data storage is practical or convenient does not justify data storage. In addition, pseudonyms or anonymous data processing are generally preferable.

1.3 Profiling

Profiling, i.e. any type of automated processing of personal data consisting in the The use of personal data for the purpose of evaluating certain personal aspects relating to a natural person on the basis of algorithms, in particular in order to analyse or predict aspects relating to the performance of work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement of that natural person, is not permitted if the processing of personal data is carried out exclusively by automated means. and that processing produces legal or similar effects for the data subject. In order to avoid wrong decisions, a check and a plausibility check by an employee must be ensured. This could be the case, for example, if applicant data is automatically compared with a previously created profile via a special program and as a result certain applicants are excluded and others are considered.

1.4 Data collection from third parties

If personal data is not collected from the employee concerned, but is procured from another company, for example, the data subject must be informed retrospectively and comprehensively about the handling of his or her data in accordance with Art. 14 GDPR. This also applies to changes to the purpose and purpose of data processing.

1.5 Special categories of personal data

Special categories of personal data may only be collected, processed or used with the consent of the data subject or, exceptionally, on the basis of explicit legal permission. According to Art. 9 GDPR, special categories of personal data are data relating to the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, genetic or biometric data, etc. of the data subject.

If such data is to be processed, additional technical and organisational measures (e.g. encryption during transport, minimal assignment of rights) must be taken to protect this particular personal data.

As a matter of principle, we reject the processing of special categories of personal data by us, unless the processing is necessary, e.g. the indication of religious affiliation for the payment of church tax.

2. Processing of personal data of customers, suppliers, partners, interested parties

2.1 Consent to data processing, Art. 6 (1) (a) GDPR

The processing of personal data of customers, suppliers, partners, interested parties may be carried out on the basis of the consent of the data subject. It is crucial that the consent meets the requirements of Art. 7 GDPR. This means that consent must be given voluntarily after the data subject has been adequately informed in a comprehensible and easily accessible form. In addition, the purpose of the processing to which the data subject consents must be clearly identifiable. The data subject must be informed that consent to data processing can be revoked at any time with effect for the future. For later evidentiary purposes, the consent must be documented. If you wish to carry out data processing on the basis of the consent of the data subject, please contact the company's data protection coordinator beforehand for advice on the requirements for legally valid consent.

The category of "consent" includes, for example, the registration of an interested party to receive an e-mail newsletter.

2.2 Data processing for the performance of a contract or for the implementation of pre-contractual measures, Art. 6 (1) (b) GDPR

The processing of personal data is also permitted if it is necessary for the performance of a contract or for the implementation of pre-contractual measures between the data subject and the controller. It must be borne in mind that the processing of personal data may only take place to the extent that this is objectively necessary.

This includes, for example, the storage and use of personal data for the delivery of goods or for the submission of an offer.

2.3 Data processing for the fulfilment of a legal obligation, Art. 6 (1) (c) GDPR

Finally, the processing of personal data is also permissible if a legal basis requires, permits or requires the processing. The type and scope of the data processing must also be objectively necessary for the requested data processing.

This category includes, for example, data processing for the purpose of customs clearance, applying for short-time work allowance or registering vehicles.

2.4 Data processing for the protection of vital interests of the data subject, Art. 6 (1) (d) GDPR

Also permissible, but hardly conceivable in our context, is the processing of personal data for the protection of the vital interests of the data subject. Since this refers to cases that affect life or health, for example in the event of a disaster, the significance for us is low.

2.5 Data processing for the protection of legitimate interests, Art. 6 (1) (f) GDPR

The processing of personal data may also take place if it is necessary to safeguard a legitimate interest of our company. Legitimate interests are usually legal or economic interests, such as the enforcement of claims or the avoidance of contractual disruptions or the use of the postal address for the purpose of sending advertising letters.

Personal data may not be processed on the basis of a legitimate interest if there are indications in the individual case that the employee's interests worthy of protection outweigh the interest in the processing. A balance between a possibly legitimate interest of our company and the interest of the employee worthy of protection must be carried out in each individual case and must be documented.

Please note that the invocation of a legitimate interest may not be made without prior consultation with the Data Protection Officer. This is because the invocation of the alternative "legitimate interest" requires an extensive and documented balancing of interests, which must meet the requirements of the supervisory authorities.

2.6 User data and website

Since data is collected and processed on our website, the data subjects must be specifically informed about this in data protection and, if applicable, cookie notices. If user profiles are created for the purpose of evaluating the usage behavior of our website (so-called tracking), the data subjects must be informed about this in the privacy policy in any case. If tracking tools are used, tracking may only be pseudonymised. If access to personal data is made possible in an area subject to registration requirements, the identification and authentication of the data subjects must be designed in such a way that adequate protection is achieved for the respective access.

3. Personal data of employees

3.1 Data processing for the employment relationship/employment relationship, § 26 para. 1 BDSG-new

For the employment relationship, personal data may be processed that is necessary for the establishment, implementation and termination of the employment relationship (§ 26 BDSG new). In this context, "necessary" means that, in addition to the suitability of the data processing to fulfil the purpose pursued by the employer (controller), there are no milder (i.e. less detrimental to the right to the protection of personal data) means.

When initiating an employment relationship, personal data of applicants may also be processed. After the rejection of an applicant, the applicant's data must be deleted in accordance with the law, taking into account evidentiary deadlines (in order to defend against possible actions based on the AGG), unless the applicant has consented in writing to the further storage for a later selection process on the basis of informed consent.

3.2 Data processing on the basis of a legal standard, § 26 para. 1 BDSG-new

The processing of employee personal data is also permitted if government legislation requires, presupposes or permits data processing. The type and scope of data processing must be necessary for the legally permissible data processing and are governed by these legal provisions. If there is legal room for manoeuvre, the employee's interests worthy of protection must be taken into account.

3.3 Collective regulations for data processing, § 26 para. 1 and 4 BDSG-new

If processing goes beyond the purpose of executing the contract, it is permissible even if it is permitted by collective regulation. The regulations must cover the specific purpose of the requested processing and must be within the framework of state data protection law.

3.4 Consent to data processing, § 26 para. 2 BDSG-new

Employee data may also be processed on the basis of the consent of the person concerned. In order for an employee's declaration of consent to be effective, it must have been given voluntarily. In this context, the "imbalance of power", which is assumed per se between employer and employee, must be taken into account appropriately for the assessment of voluntariness.

Please note that consent is invalid insofar as it would circumvent the prohibition of questions under labour law.

For evidentiary reasons, declarations of consent must always be obtained in writing or electronically/textually, or at least the consent must be properly documented. Before giving consent, the employee concerned must be informed in accordance with point III 2, (2nd transparency) of this policy.

3.5 Data processing based on legitimate interest

The processing of personal data may also take place if this is necessary for the realisation of the legitimate interests of Assured Technologies SAS. Legitimate interests are usually legally justified (e.g. assertion, exercise or defence of legal claims) or economic (e.g. valuation of companies).

Personal data may not be processed on the basis of a legitimate interest if there are indications in the individual case that the employee's interests worthy of protection outweigh the interest in the processing. A balance between a possible legitimate interest of the company and the interest of the employee worthy of protection must be carried out in each individual case and must be documented.

Please note that the invocation of a legitimate interest may not be made here either, without prior consultation with the data protection officer. This is because this invocation of the alternative "legitimate interest" also requires an extensive and documented weighing of interests, which must meet the requirements of the supervisory authorities.

3.6 Data processing for the detection of criminal offences committed by the employee concerned

The processing of personal employee data for the purpose of detecting criminal offences is permissible if there are indications that the data subject has committed a criminal offence in the employment relationship, the processing is necessary for detection and the legitimate interest of the employee(s) in the exclusion of processing does not prevail and proportionality is maintained. This means that only the investigation of criminal offences committed in the context of the employment relationship is covered, not of possible criminal offences committed outside the employment relationship.

3.7 Telecommunications and Internet

Telephone systems, e-mail addresses, intranet and Internet as well as internal social networks are provided by the company as part of its operational tasks. They are work tools and company resources. They may only be used within the framework of the applicable legal provisions as well as the applicable internal company guidelines (policy on business e-mail and Internet use). There is no general monitoring of telephone and e-mail communication as well as Internet use. To defend against attacks on the IT infrastructure or on individual users, protective measures can be implemented that block technically harmful content or analyze the patterns of attacks.

Incidentally, compliance with the requirement of purely official use of company means of communication is only checked on a random basis. Only in the event of reasonable suspicion or appearance of abuse will personal evaluations be carried out.

V. TRANSFER OF PERSONAL DATA

The transfer of personal data to third parties is only permitted on the basis of legal permission or on the basis of the consent of the data subject. The data recipient must be obliged in writing/by text to process the data received only for previously defined purposes. If the data is to be processed by the

recipient on behalf of the controller, a transfer may only take place after the conclusion of an order processing agreement that meets the requirements of the GDPR (see point VI, VI. ORDER PROCESSING). The data protection coordinator of our company has our standard data processing agreement, which may not be deviated from in principle. If adjustments are necessary, they may only be made in consultation with the Data Protection Coordinator.

If the recipient of the personal data is located outside the European Union (EU) or the European Economic Area (EEA), special measures are also required to protect the rights and interests of data subjects. Data transmission must be refrained from if the receiving entity does not have **an adequate level of data protection** or if this level cannot be established by means of special contractual clauses. The recipient must ensure a level of data protection equivalent to this Privacy Policy and European data protection laws. This does not apply if the data transfer has to take place on the basis of a legal obligation.

If personal data is transferred from a group company established in the EU or EEA to a group company based outside the EU or EEA, the data importing company is obliged to cooperate with the supervisory authority responsible for the data exporting company in all requests and to comply with the findings of the supervisory authority with regard to the data transferred.

In the event of an alleged breach of this Privacy Policy by a data-importing group company established in a third country, the data-exporting group company established in the EU or the EEA undertakes to assist the data subject whose data has been collected both in establishing the facts and enforcing its rights under this Privacy Policy against the data importing company Ensure. In addition, the data subject is also entitled to assert his or her rights vis-à-vis the data-exporting group company. In the event of an alleged breach, the data-exporting company must provide proof to the data subject that a breach of this data protection policy is not attributable to the data-importing group company in a third country in the event of further processing of the data received.

In the event of a transfer of personal data from a group company with its registered office in the EU or the EEA to a group company with its registered office in a third country, the data transmitting entity shall hold the data subject whose personal data was collected liable for liability purposes as if the data transmitting entity had committed the breach in the event of attributable breaches of this data protection policy by the group company based in a third country. The place of jurisdiction is the competent court at the registered office of the data exporting entity.

VI. ORDER PROCESSING

1. Order processing

Order processing occurs when a contractor is commissioned with the processing of personal data without being given responsibility for the associated business process and without the contractor itself deciding on the purposes and means of data processing.

2. Prior information of the data protection officer

If external service providers (processors) are to be commissioned for the first time with the processing of personal data or individual processing steps or with activities in which they are given the opportunity to gain knowledge of personal data, the data protection coordinator and the data protection officer must be **appointed before the commission.** by submitting a draft contract that satisfies the requirements of Art. 28 GDPR and the criteria for the order control that has been carried out or is provided for below. The Company has a standard data processing agreement to be used in these cases.

3. Selection of the service provider

The service providers must be selected carefully. The selection must be documented and must take into account in particular the following aspects:

- Professional suitability of the contractor for the specific handling of data
- Implementation of technical and organizational measures for data security
- Provider's experience in the market

- other aspects that indicate the reliability of the provider, such as data protection documentation, willingness to cooperate, response times, etc.

4. Conclusion of a data processing agreement (DPA)

If a service provider is to process personal data on our behalf, it is necessary to conclude a contract for order processing (DPA) in advance. Our company has a standard data processing agreement, which is to be applied in all cases where a data processing relationship exists, after consultation with the data protection coordinator and the data protection officer, in order to ensure that the legal requirements for order processing are met. You will receive our standard DPA from the Data Protection Coordinator. Deviations from the provisions of this bill are generally not permitted. Should a contractual partner wish to make changes or additions in individual cases, these must be discussed in advance with the data protection coordinator and the data protection officer.

A data processing relationship also exists if our company should process personal data on behalf of a controller. This constellation is likely to occur rather rarely, but cannot be ruled out in principle.

In the context of order processing, the Contractor may only act in accordance with the instructions of the Client or in accordance with the contractual provisions of the Data Protection Agreement. The obligations of the Contractor arise on the one hand from the DPA and on the other hand from the law. The instructions of the client must be documented.

Please note: Only those processors/contractors may be engaged that provide sufficient guarantees that appropriate technical and organizational measures are implemented in accordance with the requirements of the GDPR and that the protection of the rights of the data subject is ensured. The contractor must be regularly inspected with regard to these technical and organisational measures, and the result of the inspection must be documented. The presentation and detailed explanation of the technical and organisational measures that the Contractor has implemented in its company to protect the personal data it processes on behalf of the Contractor must be attached to the Data Processing Agreement. Please take sufficient care to check the technical and organizational measures. If you need assistance, please contact our company's Data Protection Coordinator and/or Data Protection Officer.

Furthermore, the data processing agreement must describe the subject matter and duration of the order as well as the scope, type and purpose of the intended processing or use of data, the type of data and the circle of data subjects for each individual case. Sufficient care must also be taken in this regard.

In addition to the explicit regulation of the contractor's obligations, the rights and obligations of the controller, an explicit regulation on the admissibility of subcontracting relationships must be made. Since we, as the client, are also liable for the selection of subcontractors, special attention must be paid here. Under no circumstances may subcontractors be accepted without further examination and in general.
It must be ensured that the contractual relationship between the processor and the other processor (subcontractor) corresponds to the contractual relationship between us and our processor. Therefore, prior consultation with the Data Protection Coordinator and/or the Data Protection Officer is required. Subcontractors must be listed with name and address.

In addition to the persons authorised to issue instructions at Assured Technologies SAS (if we are the controllers), it is of great importance to name the persons authorised to receive instructions from the respective processor. Persons other than these named persons do not have the right to issue instructions or are not entitled to receive instructions. Therefore, great attention must be paid to the selection of persons.

5. Forms in the context of order processing

The Company provides various forms that must be used in the various situations that arise in the context of order processing in order to comply with the documentation obligation required by law. These documents concern:

- the approval of subcontractors by the management
- the documentation of changes in the persons authorised or recipient of instructions
- Changes to the designated data protection officer
- Reporting form for data protection or IT security incidents

The forms are stored in MS Teams WIKI.

VII. RECORD OF PROCESSING ACTIVITIES (VVT)

Our company is obliged to keep a record of all processing operations, i.e. all procedures within which personal data is processed. Careful maintenance of this register is a prerequisite for accountability for compliance with the principles governing the processing of personal data. The template for the record of processing activities (description of the procedure) is available from the Data Protection Coordinator.

Each department is responsible for ensuring that an overall overview of the procedures is first drawn up for all procedures of the respective department, as well as that each procedure is described.

In each department, (at least) one person is responsible for gathering the necessary information on the procedures of the respective department and documenting them in accordance with the requirements of Art. 30 GDPR. If there is any ambiguity regarding the information required by law, the data protection officer and, if necessary, the data protection coordinator should be consulted. A copy of the list of procedures must be provided to the data protection officer. As soon as the directory is updated, these updates must be made available to it without delay.

The record of processing activities is of central importance in data protection. Therefore, we ask you to take the utmost care in creating the directory and updating it permanently.

At the request of the supervisory authority, we are obliged to provide this list to the supervisory authority. Please note that without the involvement of the data protection officer and without explicit internal regulations, no communications, information, etc. from employees may be sent to external bodies. The Data Protection Officer and the Data Protection Coordinator are solely responsible for communication with supervisory authorities.

VIII. DATA PROTECTION IMPACT ASSESSMENT (DPA)

1. Data Protection Impact Assessment at High Risk to Rights and Freedoms

If a data processing operation in our company is likely to result in a high risk to the rights and freedoms of natural persons, we, or each specialist department, are obliged to carry out a so-called data protection impact assessment (DPIA) for the procedure for which it is responsible. In particular, a DPIA must be carried out in the case of the use of new technologies. The DPIA must be carried out not only in the case of risks to the protection of personal data, but also in the event of risks such as: physical, material or non-material damage due to the destruction, loss or alteration of personal data, limitation of rights, discrimination, identity theft, fraud, financial losses, unauthorised removal of pseudonymisation, damage to reputation, loss of confidentiality of data subject to professional secrecy as well as other significant economic or social disadvantages for natural persons. The data protection impact assessment has to meet certain requirements and follows a defined procedure. Therefore, a Data Protection Impact Assessment Team (DPIA Team) has been set up, which is responsible for the DPIA.

2. Timing of the Data Protection Impact Assessment

The data protection impact assessment must be carried out prior to the respective processing that carries the high risk described above. This means that a data protection impact assessment must be carried out before the introduction of new software, before the introduction of new processes, before the introduction of new technologies, before the activation of new features of existing software, before the expansion of the categories of processed data, etc. Please note that the DPIA must in any case be carried out in advance of the processing activity.

3. Data Protection Impact Assessment Team

A permanent DPIA team has been set up to carry out the DPIA. The team consists of the following people:

- Data protection supervisor
- Data Protection Coordinator
- Head of Finance

The DPIA team will meet to conduct a DPIA if necessary. If the need to carry out a DPIA becomes apparent, the appointment is coordinated by the data protection coordinator, who invites the other team members and informs them further if necessary.

4 Involvement of Data Protection Officers

The data protection officer must be informed in advance and consulted on the implementation of the data protection impact assessment as well as on the question of whether and when processing may involve a high risk for data subjects (Art. 35 (2) GDPR).

IX. PROCUREMENT OF HARDWARE AND SOFTWARE, INTRODUCTION OF NEW PROCEDURES

1. Procurement of hardware and/or software

The procurement of hardware and software is generally carried out at the request of the person or department responsible for the processing by the central IT procurement department in accordance with the existing regulations. Please note that a DPIA may have to be carried out in advance.

2. Privacy by Design und Privacy by Default

Already in the selection of hardware and software, the principles of guaranteeing data protection by design and by data protection-friendly default settings (privacy by design and privacy by default) must be observed as supporting criteria. Data protection must be integrated into the specifications and architecture of data processing systems from the outset in order to facilitate compliance with the principles of privacy and data protection, in particular the principle of data minimisation.

3. Informing the data protection officer at an early stage

If a new procedure for the processing of personal data is to be introduced with the procurement, in particular a procedure supported by software, the data protection officer must be informed in good time in advance by the requesting body. The procurement may only take place after the opinion of the Data Protection Officer, who in this case also advises on whether the implementation of a DPIA is necessary (see above, VIII. DATA PROTECTION IMPACT ASSESSMENT).

X. CONFIDENTIALITY AND SECURITY OF PROCESSING

1. Confidentiality of processing

Personal data is subject to data secrecy. Any employee is therefore prohibited from unauthorised processing. Any processing carried out by an employee without being entrusted with it in the performance of his or her duties and without complying with the principles set out in points III (III. GENERAL PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA AND DATA SECURITY) AND IV (IV. LAWFULNESS OF THE PROCESSING OF PERSONAL DATA) OF THIS Policy is unauthorised.

Please remember: In principle, employees may only have access to personal data if and to the extent necessary for their respective tasks. This requires a careful division and separation of roles and responsibilities as well as their implementation and maintenance within the framework of authorization concepts.

2. Commitment to data secrecy

Employees may not use personal data for their own private or commercial purposes, transmit it to unauthorized persons or make it accessible to it in any other way. Supervisors must inform their employees of the obligation to maintain data secrecy at the beginning of the employment relationship. At the beginning of their employment relationship, or at any subsequent time, each employee must sign a declaration of commitment to data secrecy, which will be made available by the Human Resources Department, otherwise they may not be able to work for the intended purpose or be hired. The HR department and the respective supervisor are jointly responsible for ensuring that a declaration of commitment is issued by each employee assigned. Parallel to the declaration of commitment, the employee must be informed about the data protection regulations, the rules and instructions for conduct.

3. Security of processing

Personal data must be protected at all times against unauthorised access, unlawful processing or disclosure, as well as against loss, falsification or destruction. This applies regardless of whether the data processing is carried out electronically or in paper form. Prior to the introduction of new data processing procedures, in particular new IT systems, technical and organisational measures for the protection of personal data must be established and the DPIA described in point VIII of this Directive (VIII DATA PROTECTION IMPACT ASSESSMENT) must be carried out. The technical and organizational measures must be based on the state of the art, the risks arising from the processing and the need for protection of the data. In particular, the responsible department can consult the IT employee responsible for information security or the data protection coordinator. The technical and organizational measures for the protection of personal data are part of the company-wide information management and must be continuously adapted to technical developments and organizational changes.

In order to maintain the availability, confidentiality and integrity of the data as well as the resilience of the data processing systems, a general IT security concept has been drawn up. The concept is based on the previously prepared protection needs assessment and risk analysis. This concept is decisive for all further proceedings. The IT department is responsible for creating the concept. In addition to this directive, there are supplementary regulations that concern in particular the measures to be taken to implement the data security requirements of Art. 32 GDPR.

XI. PRIVACY CONTROL

1. Data Protection Audits

In order to ensure a high level of data protection in our company, relevant processes are reviewed by regular audits by internal bodies or by external auditors. If potential for improvement is identified, immediate remedial action must be taken.
The findings of the audit must be documented. Unless the data protection officer has carried out the audit, the documentation must be handed over to the data protection officer, the company management and the specialist responsible for the respective process. An audit is successfully completed when all measures documented in the report have been implemented. If necessary, follow-up audits are carried out by reviewing the implementation of the initial audit's recommendations.
The internal data protection team is responsible for the implementation and commissioning of regular audits.

2. Enquiries with authorities

Upon request, the results of data protection checks or audits will be communicated to the supervisory authority. Again, this notification will only be made by the Data Protection Officer or on the instructions of the Data Protection Officer.

XII. DATA PROTECTION OFFICER, DATA PROTECTION COORDINATOR, DATA PROTECTION TEAM

1. Data security engineer

In accordance with Article 37 of the GDPR, Assured Technologies SAS has appointed a Data Protection Officer (DPO) as well as an additional Data Protection Coordinator (DSK), who also takes over the absence of the DPO. The Data Protection Officer can be reached at:

Brigitte Jordan
REVIDATA GmbH
datenschutz@revidata.org
Phone: +49 211 65584395

The DPO performs the tasks assigned to it by law (Art. 39 GDPR) by applying its specialist knowledge and professional qualifications without instructions.

2. Responsibilities of the Data Protection Officer

The Data Protection Officer informs and advises the company's management and employees regarding their data protection obligations. It is responsible for monitoring compliance with data protection rules and the personal data controller's policies, including the allocation of responsibilities, awareness raising and training of employees. In the case of high-risk data processing, the data protection officer advises the controller on the assessment of the risk.

3. Position of the Data Protection Officer

The Data Protection Officer reports directly to the company's top management (see Art. 38 para. 3, last sentence). It must be involved in all data protection issues at an early stage and is comprehensively supported by both the company management and the employees in the performance of their tasks.

4. Data Protection Coordinator

In addition to the data protection officer, the company has appointed an internal data protection coordinator (DSK). The Data Protection Coordinator represents the Data Protection Officer in the event of the latter's absence, and assists and assists the Data Protection Officer. In this function, the Data Protection Coordinator is assigned to the Data Protection Officer. The Data Protection Coordinator informs the Data Protection Officer of any data protection issues and problems that have arisen locally. It collects information on the procedures used in its area of responsibility and forwards the report to the Data Protection Officer.

He is also a member of the various internal committees or teams formed for data protection, such as the DPIA team. He can be reached at:

Adam Gawrys
E-mail adam@assuredtechnologies.com

5. Data Protection Team

In addition, an internal data protection team has been put together. The task of this internal team is to coordinate the essential tasks and requirements in connection with the development of a data protection management system, to delegate tasks to the competent and responsible persons and to take care of some of the tasks themselves.

The internal data protection team is made up of the following persons:

- Data Protection Coordinator

6. Confidentiality of requests

Any employee can contact the Data Protection Officer directly with any information, suggestions or complaints . As a matter of principle, the data protection officer maintains absolute confidentiality, unless the employee wishes to be passed on and informed about his or her request.

XIII. RIGHTS OF DATA SUBJECTS

The so-called rights of the data subject are rights of the person affected by a data application vis-à-vis the controller. Any data subject may assert his/her rights against the controller at any time. If a data subject asserts one or more of these rights, the immediate processing of the internally responsible area and the immediate information of the DPO and the DSK must be ensured. The exercise of these rights is free of charge for the data subject. This means, for example, that no expense allowance can be demanded for the provision of information or that it can be claimed for the deletion

Please make sure that the internally defined process for processing data subject rights (see point XIV, XIV. DEALING WITH REQUESTS FROM DATA SUBJECTS) is adhered to. The data protection officer must be consulted in the event of an assertion of rights by data subjects. In the following, we present the so-called rights of data subjects, so that in the event of an inquiry or assertion, you are at least fundamentally informed about the existence of these rights:

1. Right to confirmation

Every data subject has the right to request an explanation as to whether personal data about him or her is being processed by us.

2. Right of access

Every data subject also has the right to obtain information regarding the personal data stored about him/her, as well as the further information listed below and to obtain a copy of the data in accordance with Art. 15 GDPR. This means that the data subject has the right to information about:

- the purposes of processing
- the **categories** of personal data that are processed
- the **recipients** or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations
- if possible, the envisaged **period** for which the personal data will be stored or, if this is not possible, the criteria used to determine this period
- the existence of a **right to rectification or erasure** of personal data concerning you or to restriction of processing or a right to object to such processing
- the existence of a **right to lodge** a complaint with a supervisory authority
- if the personal data is not collected from you as a data subject: any available information about the **origin of the data**
- the existence of **automated decision-making**, including profiling, pursuant to Art. 22(1) and (4) GDPR and, at least in these cases, meaningful information about the logic involved, as well as the scope and intended effects of such processing for the data subject.

3. Right to rectification and completion

Pursuant to Art. 16 GDPR, every data subject has the right to request the rectification of personal data concerning him/her. In addition, each data subject has the right to request the completion of incomplete personal data, taking into account the purposes of the processing.

4. Right to erasure (to be forgotten)

In accordance with Art. 17 GDPR, every data subject also has the right to request that data concerning him or her be erased without undue delay, provided that one of the following grounds applies and insofar as the processing is not necessary:

- The personal data has been collected or otherwise processed for purposes for which it is no longer necessary.
- The data subject withdraws his or her consent, on which the processing was based pursuant to Art. 6(1)(a) GDPR or Art. 9(2)(a) GDPR, and there is no other legal basis for the processing.
- The data subject objects to the processing pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR.
- The personal data has been unlawfully processed.
- The erasure of the personal data is necessary for compliance with a legal obligation under Union law or the law of the Member States to which the controller is subject.
- The personal data was collected in relation to information society services offered in accordance with Article 8(1) of the GDPR.

Statutory retention periods and deletion dates are based on the company's deletion concept published within the company.

5. Right to restriction of processing

Furthermore, every data subject has the right to obtain from us the restriction of processing if one of the following conditions applies:

- the accuracy of the personal data is disputed by the data subject, for a period enabling us to verify the accuracy of the personal data
- the processing is unlawful, but the data subject opposes the erasure of the personal data and requests the restriction of the use of the personal data instead;
- we no longer need the personal data for the purposes of the processing, but the data subject needs it for the establishment, exercise or defence of legal claims (including legal claims against us)
- the data subject has objected to the processing pursuant to Art. 21 (1) GDPR, but it is not yet clear whether our legitimate grounds outweigh the interests of the data subject worthy of protection.

6. Right to data portability

Furthermore, every data subject has the right to receive the personal data concerning him/her, which he/she has provided to us, from us in a structured, commonly used and machine-readable format. In addition, it has the right to request the transfer of this data from us to another controller, provided that the processing is based on consent pursuant to Art. 6 (1) (a) GDPR or Art. 9 (2) (a) GDPR or on a

contract pursuant to Art. 6 (1) (b) GDPR **and** the processing is carried out by automated means, and where the processing is not necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us and provided that it does not adversely affect the rights and freedoms of other persons. It should be borne in mind that this right only applies to data provided by the data subject himself/herself.

7. Right to object

Finally, every data subject has the right to object at any time to the processing of his or her personal data based on Art. 6 (1) (e) or (f) GDPR. This also applies to profiling based on these provisions.

Please note: In the event of an objection, personal data may no longer be processed, unless there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or the processing of the data serves to assert, exercise or defend legal claims. If personal data is processed for the purpose of direct marketing, the data subject has the right to object at any time to the processing of his or her data for the purpose of such advertising. This also applies to profiling insofar as it is related to such direct marketing. In addition, the data subject has the right to object to the processing of his or her personal data carried out by us for scientific or historical research purposes or for statistical purposes pursuant to Art. 89 (1) GDPR, unless such processing is necessary for the performance of a task carried out in the public interest.

8. Right to withdraw consent

In addition, any data subject has the right to withdraw his or her consent to the processing of personal data at any time and without justification. The revocation is only effective for the future.

9. Right to lodge a complaint with a supervisory authority

Furthermore, pursuant to Art. 77 GDPR, every data subject has the right to lodge a complaint with the supervisory authority if he or she believes that the processing of personal data concerning him or her violates the GDPR.

XIV. DEALING WITH REQUESTS FROM DATA SUBJECTS

1. Identity verification

When processing requests from data subjects, the identity of the requester must first be established beyond doubt. If there are reasonable doubts as to the identity, additional information may be requested from the applicant in order to establish the identity. Please make sure, however, that it is established beyond doubt that the person making the request is actually the data subject and is therefore entitled to make the request.

2. Provision of information

Information may only be provided in writing to the unequivocally identified data subject, unless the data subject has submitted the request for information electronically. In this case, the information may also be provided electronically. The information must be accompanied by a copy of the data of the data subject, which, in addition to the data available on the person, must also include the recipients of the data, the purpose of storage and all other information required by law in accordance with Art. 15 GDPR. It must enable the data subject to assess the lawfulness of the processing for himself/herself. At the special request of the data subject, the data will be made available in a structured, commonly used and machine-readable format. The responsible IT department determines the standard to be provided for this purpose.

3. Reaction deadline

The person concerned must be informed, within one month at the latest, of all measures taken at his or her request.

4. Internal Responsibility

All inquiries and requests from data subjects must be forwarded immediately to the internal data protection coordinator. The provision of information and response to enquiries may only be carried out by the persons expressly authorised to provide information internally in cooperation with the data protection officer.

XV. DATA PROTECTION INCIDENTS ("DATA BREACHES")

1. Deadline for reporting a data breach

In the event of a personal data breach, our company is obliged to report the personal data breach to the competent supervisory authority as soon as possible, but within 72 hours of becoming aware of it. Therefore, any such data breach that becomes known internally must be immediately reported to the Data Protection Coordinator and the Data Protection Officer, who will act in accordance with the internal crisis response plan.

2. Internal reporting of the data breach

The internal report must contain all relevant information necessary to clarify the facts, in particular the receiving entity, the data subjects, as well as the nature and scope of the (unlawfully) transmitted data.

We expressly ask you to report data protection incidents as quickly and transparently as possible at all times and therefore exclude any sanctioning of the reporting persons.

3. Data breaches

Personal data breach (data breach) means a breach of security that results in the destruction, loss, alteration, or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, whether accidental or unlawful. Data breaches include a wide variety of incidents, such as, but not limited to: attacks by hackers or Trojans, software errors, hardware failures, the loss of smartphones, notebooks, tablets, or, for example, the handwritten note of the access data to the account or a USB stick with internal company documents, etc. If there is uncertainty as to whether a data breach has occurred, the data protection officer must be consulted.

4. Fulfilment of information obligations

The fulfilment of the existing obligation to provide information to the supervisory authority is carried out exclusively by the data protection officer. The data subjects who are also to be informed about the incident will be informed by the management, whereby the data protection officer will be consulted.

XVI. ACCOUNTABILITY AND SANCTIONS

1. Accountability

Each and every employee of our company is responsible for compliance with this Privacy Policy as well as data protection laws. It must be possible to demonstrate compliance with the requirements of this Directive at all times (accountability). Particular attention must be paid to the traceability and transparency of the measures taken, for example via associated documentation.

2. Sanctions

A negligent or even wilful breach of this policy may result in consequences under employment law, including dismissal without notice or notice of termination. Criminal sanctions and civil penalties may also be considered.

XVII. In effect

This policy comes into force on 06.10.2022.