DATA PROTECTION POLICY EU

Table of Contents

Reviewed:
October 2019

This policy will be reviewed on a regular basis to evaluate continued relevance and to monitor compliance.

DATA PROTECTION POLICY EU

1 Aim of the Policy

The Garant Group considers the safeguarding of data protection rights as part of its social responsibility.

In some countries and regions, such as the European Union, legislators have defined standards for protecting the data of natural persons (“personal data”), including the requirement that such data may only be transferred to other countries if the local law applicable at the place of destination provides for an adequate level of data protection.

This Data Protection Policy EU establishes uniform and suitable data protection standards within the Group for:

» (a) processing personal data in regions such as the EU / the European Economic Area (EEA) (hereinafter referred to collectively as the “EU”) and » (b) cross-border transmission of personal data to Group Companies outside the EU (including subsequent data processing there).

To this end, this Policy enacts binding rules for processing personal data from the EU within the Garant Group. These rules provide adequate guarantees for the protection of personal data outside the EU and are referred to as (“Binding Corporate Rules - BCR”) for the Garant Group.

2 Scope

This Data Protection Policy EU applies to Garant, its controlled Group Companies (hereinafter Group Companies) and its employees and members of managing bodies. “Controlled” in this instance means that Garant Group may enforce the adoption of this policy directly or indirectly, on the basis of its voting majority, majority management representation, or by agreement.

The Policy applies to fully or partially automated processing of personal data, as well as manual processing in filing systems unless national laws provide for a broader scope. The Policy also applies to all employee data1 in hard-copy format in Lithuania.

The Policy applies to the processing of personal data:

» third country companies that receive data from the EU

» (a) from Group Companies and their subsidiaries that are established in the EU or another country to which this Policy can be extended (“EU-based companies”),

» (b) from Group Companies established outside the EU, if they offer goods or services to natural persons within the EU and/or monitor the behavior of natural persons within the EU (“third country companies with offers for the EU”) or » (c) of Group Companies established outside the EU, if they have received personal data directly or indirectly from companies that are subject to the Policy under a) or b), or if such data has been disclosed to them (“third country companies that receive data from the EU”).

Processing outside the EU is further referred to in this Policy as processing in a third country.

The Group Companies that take part in, or are subject to, processing by third country companies are listed in the further applicable regulation “List of Group Companies bound by the Data Protection Policy EU”.

This Policy can be extended to countries outside the EU. In countries where the data of legal entities is protected in the same manner as personal data, this Policy also applies in the same manner to the data of legal entities.

3 Legal Enforceability within the Garant Group

The rules and provisions of this Policy are binding to all Group Companies operating within its scope of application. In addition to the applicable EU legislation and national data protection laws, the Group Companies as well as their management and employees are therefore responsible for compliance with this Policy.

Reviewed:
October 2019

This policy will be reviewed on a regular basis to evaluate continued relevance and to monitor compliance.

As far as it is not otherwise stipulated by legal requirements, Group Companies are not entitled to adopt regulations that deviate from this Policy.

4 Relationship to Legal Requirements

This Policy does not replace EU legislation and national laws. It supplements the national data protection laws. These regulations and laws shall take priority if compliance with this Policy would result in a violation of national law. The content of this Policy must also be observed in the absence of corresponding national laws.

If compliance with this Policy would result in a violation of national law, or if regulations that deviate from this Policy are required under national law, this must be reported to the Sales Quality Officer I Officer Corporate Data Protection and the central compliance organization for the purposes of data protection law monitoring. In the event of conflicts between national laws and this Policy, the Sales Quality Officer I Officer Corporate Data Protection and the central compliance organization will work with the responsible Group Company to find a practical solution that fulfills the purpose of this Policy.

5 General Principles for the Processing of Personal Data

5.1. Lawfulness

Personal data must be processed in a lawful manner and in good faith. Data Processing may only take place if and insofar as a sufficient legal basis exists for the processing activity. This also applies to data processing between Group Companies. The mere fact that both, the transferring and receiving Group Company are affiliated to Garant Group does not readily constitute such legal basis.

The processing of personal data is lawful if one of the following circumstances for authorization under Section 5.2 or 5.3 applies. Such circumstances for permissibility are also required if the purpose of processing the personal data is to be changed from the original purpose.

5.2. Legal basis Customer and Partner Data Data Processing for a contractual relationship

5.2.1.Personal data of the prospective customer, customer, or partner can be processed to establish, perform and terminate a contract. This also includes advisory services for the customer or partner under the contract if this is related to the contractual purpose.

Prior to a contract, personal data can be processed to prepare bids or purchase orders or to fulfill other requests of the prospective customer relating to contract conclusion. Prospective customers can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by the prospective customers must be complied with.

5.2.2.Data processing for advertising purposes

If the data subject contacts a Group Company with a request for information (e. g. request to receive information material about a product), processing of personal data to meet this request is permitted. Customer loyalty or advertising measures are subject to further legal requirements. Personal data can be processed for advertising purposes or market and opinion research, provided that this is consistent with the purpose for which the data was originally collected. The data subject must be informed in advance about the use of his/her personal data for advertising purposes. If personal data is collected only for advertising purposes, the data subject can choose whether to provide this data. The data subject shall be informed that providing data for this purpose is voluntary. As part of the communication process, consent should be obtained from the data subject. When giving consent, the data subject should be given a choice among available forms of contact, such as e-mail and phone (consent see Section 5.2.3). If the data subject objects to the use of his/her data for advertising purposes, it can no longer be used for these purposes and must be restricted or blocked from use for these purposes. Any other restrictions from specific countries regarding the use of data for advertising purposes must be observed.

5.2.3.Consent to data processing

Personal data can be processed following the consent by the data subject. Before giving consent, the data subject must be informed in accordance with this Data Protection Policy EU. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can also be given verbally. The granting of consent must be documented.

5.2.4. Data processing pursuant to legal authorization or obligation

Reviewed:
October 2019

This policy will be reviewed on a regular basis to evaluate continued relevance and to monitor compliance.

The processing of personal data is also permitted if national legislation requests, requires, or allows this. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions.

5.2.5. Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary for a legitimate interest. Legitimate interests are generally of a legal (e. g. collection of outstanding receivables) or commercial nature (e.g. avoiding breaches of contract). Processing cannot take place on the basis of a legitimate interest if, in a specific instance, the data subjects' interests worthy of protection outweigh the legitimate interests in processing. Before data is processed, it is necessary to determine whether there are interests worthy of protection.

5.3. Legal Basis Employee Data

5.3.1. Data Processing for the employment relationship

For employment relationships, personal data can be processed if needed to establish, perform and terminate the employment relationship. Personal data of candidates can be processed to help decide whether to enter into an employment relationship. If the candidate is rejected, his/ her data must be deleted in observance of the required retention period, unless the candidate has agreed to remain on file for a future selection process. Consent is also needed to use the data for further application processes or before sharing the application with other Group Companies. In the existing employment relationship, data processing must always relate to the purpose of the employment relationship if none of the following circumstances for authorized data processing apply.

If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national laws have to be observed. In cases of doubt - where permitted - consent must be obtained from the data subject.

A legal basis as listed below must be met to process personal data that is related to the employment relationship but was not originally part of creating, performing or terminating the employment relationship (employee data).

5.3.2. Data processing pursuant to legal authorization or obligation

The processing of employee data is also permitted if national legislation requests, requires, or allows this. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions. If there is some legal flexibility, the protective interests of the employee must be taken into consideration.

5.3.3. Collective agreement on data processing

If a data processing activity exceeds the purposes of fulfilling a contract, it may still be lawful if authorized through a collective agreement. The agreements must cover the specific purpose of the intended data processing activity, and must be drawn up within the parameters of EU and national legislation.

5.3.4. Consent to data processing

Employee data can be processed upon consent of the data subject. Declarations of consent must be submitted voluntarily. No penalties can be imposed for refusal of consent. Involuntary consent is not valid. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. If, exceptionally, circumstances do not permit this, consent may be given verbally. Their granting must be in any case properly documented. Before giving consent, the data subject must be informed in accordance with this Data Protection Policy EU.

5.3.5. Data processing pursuant to legitimate interest

Employee data can also be processed if it is necessary for a legitimate interest of a Group Company. Legitimate interests are generally of a legal (e. g. filing, enforcing or defending against legal claims) or a commercial nature (e.g. acceleration of business processes, valuation of companies). Before data is processed, it must be determined whether there are interests worthy of protection. Personal data can be processed based on a legitimate interest if the interests worthy of protection of the employee do not outweigh the interest in processing.

Control measures that require the processing of employee data beyond performance of the employment relationship (e. g. performance checks) cannot be taken unless there is a legal obligation or justified reason to do so. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. To this end, the legitimate interests of the Group Company

Reviewed:
October 2019

This policy will be reviewed on a regular basis to evaluate continued relevance and to monitor compliance.

in performing the control measure (e. g. compliance with legal provisions and internal company rules) must be weighed against any protective interests that the employee affected by the measure may have in exclusion of the measure. The measures may only be taken if they are appropriate in the specific case. The legitimate interest of the Group Company and any interests worthy of protection of the employee must be identified and documented before any measures are taken. Moreover, any additional requirements under applicable law (e.g. rights of co-determination for the employee representatives and rights of the data subjects to obtain information) must be taken into account.

5.4. Processing of highly Sensitive Data

The processing of highly sensitive personal data must be expressly permitted or prescribed under national law. Processing of such data by the Group Company may be permitted in particular if the data subject has given his express consent, if the processing is necessary for asserting, exercising or defending legal claims with respect to the data subject or if processing is necessary for the controller to fulfill its rights and responsibilities in the area of labor and employment law. If there are plans to process highly sensitive personal data, the Sales Quality Officer I Officer Corporate Data Protection must be informed in advance.

5.5. Automated individual Decision Making (possibly incl. Profiling)

The data subjects can be subject to a fully automated decision that could have a legal or similarly negative impact on them only if this is necessary to conclude or perform a contract, or if the data subject has granted consent. This automated decision can include profiling in some cases, i.e. the processing of personal data that evaluates individual personality characteristics (e.g. creditworthiness). In this case, the data subject must be notified about the occurrence and outcome of an automated individual decision and be given the opportunity to have an individual review performed by a controller.

5.6. Duty of Information/Transparency

The responsible department must inform the data subjects of the purposes and circumstances of the processing of their personal data in a concise, transparent, intelligible and easily accessible form and in clear and plain language. The requirements of the Sales Quality Officer I Officer Corporate Data Protection and Data Compliance must be observed. This information must be given whenever the personal data is collected for the first time. If the Group Company receives the personal data from a third party, it must provide the information to the data subject within a reasonable period after obtaining the data, unless » the data subject already has the information or » it would be impossible or » extremely difficult to provide this information.

5.7. Purpose Limitation

Personal data may be processed only for the legitimate purpose that was defined before collection of the data. Subsequent changes to the purpose of processing are only permissible subject to the requirement that the processing is compatible with the purposes for which the personal data was originally collected.

5.8. Data Minimization

Any processing of personal data must be limited, both quantitatively and qualitatively, to what is necessary for the achievement of the purposes for which the data is lawfully processed. This must be taken into account during the initial data collection. If the purpose permits, and the effort is in proportion to the objective pursued, anonymized or statistical data must be used.

5.9. Accuracy of Data

The personal data stored must be objectively correct and, if necessary, up to date. Appropriate measures must be adopted to ensure that incorrect or incomplete data is deleted, corrected, supplemented or updated.

5.10. Privacy by Design

The principle of “Privacy by Design” aims to ensure that departments define state-of-the-art internal strategies and adopt measures to integrate data protection principles into the specifications and architecture of business models/processes and IT systems for data processing from the very beginning during the phase of conceptualization and technical design. In accordance with the principle of “Privacy by Design,” the procedures and systems for processing personal data must be designed so that their default settings are restricted to the data processing necessary to fulfill the purpose. This includes the processing scope, storage period, and accessibility. Further measures could include:

Reviewed:
October 2019

This policy will be reviewed on a regular basis to evaluate continued relevance and to monitor compliance.

» pseudonymization of personal data as soon as possible » providing transparency about the functions and processing of personal data » allowing the data subjects to decide on the processing of their personal data » enabling the operators of procedures or systems to devise and enhance security features.

Every Group Company shall implement and maintain appropriate technical and organizational measures throughout the entire life cycle of its processing activities, in order to ensure that the above principles are complied with at all times.

5.11. Deletion & Anonymization

Personal data may only be stored for as long as it is necessary for the purpose for which the data is being processed. This means that personal data must be deleted or anonymized as soon as the purpose of its processing has been fulfilled or otherwise lapses, unless documentation or retention obligations continue to apply. Those responsible for individual procedures must ensure the implementation of the deletion and anonymization routines for their procedures. Each system must have a manual or automated deletion routine. Deletion requests from data subjects through deletion or removal of the personal identifiers must be technically feasible in the systems. Requirements that Garant Group imposes for the performance of deletion routines (such as software tools, handout for the implementation of deletion concepts, documentation requirements) must be observed.

5.12. Security of Processing

Personal data must be protected from unauthorized access and unlawful processing or transfer, as well as from accidental loss, alteration or destruction. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing and the need to protect the data.

The technical and organizational measures relevant to data protection must be documented by the controller in the context of the Data Protection Impact Assessment and the Record of Processing Activities.

In particular, the responsible department must consult with its Business Information Security Officer (BISO), its Information Security Officer (ISO) and its Data Protection Network. The requirements for the technical and organizational measures for protecting personal data are part of the Corporate Information Security Management and must be continuously adjusted in accordance with technical developments and organizational changes.

5.13. (Further) Transmission outside the Garant Group

Transmission of personal data to recipients outside or inside the Group Companies is subject to the authorization requirements for processing personal data under this Section 5. The data recipient must be required to use the data only for defined purposes.

In the event of a cross-border transmission of personal data (including granting access from another country), the relevant national requirements for the transfer of personal data abroad must be fulfilled. In particular, personal data from the EU may only be processed outside the Group Companies in a third country if the recipient can prove that it has a data protection level equivalent to this Policy. Suitable tools can be:

» Agreement on EU standard contractual clauses,

» Participation of the recipient in an EU-accredited certification system for ensuring an adequate level of data protection, or

» Recognition of binding corporate rules of the recipient to create an adequate level of data protection by the responsible supervisory authorities.

Transfers of personal data to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

In the event of conflicts between these and public authority requirements, Garant Group will work with the responsible Group Company to find a practical solution that fulfills the purpose of this Policy.

All duties listed in this Section 5 are third party beneficiary rights for the data subject.

Reviewed:
October 2019

This policy will be reviewed on a regular basis to evaluate continued relevance and to monitor compliance.

6 Data Protection Impact Assessment

Group Companies shall, when introducing new processings, or in the event of a significant change to an existing processing, particularly through the use of new technologies, assess whether this processing poses a high risk to the privacy of data subjects. The nature, scope, context and purpose of the data processing must be taken into account. As part of the risk analysis, the responsible department carries out an assessment of the impact of the planned processing on the protection of personal data (Data Protection Impact Assessment). Provisions established by Garant Group for performing this assessment (such as software tools, instructions on the performance of an evaluation) must be observed.

7 Documentation of Data Processing Procedures

Each Group company must document the procedures in which personal data is processed in a Record of Processing Activities. Provisions established by Garant Group for documentation (such as software tools and instructions on documentation) must be observed.

8 Processing on Behalf

8.1. General

Processing on behalf means that a contractor processes personal data as a service provider (processor) on behalf of and according to the instructions of the controller. In these cases, an agreement on processing on behalf must be concluded both with external processors as well as among Group Companies within the Garant Group. The controller retains full responsibility for the correct performance of the data processing.

The provisions of Section 8.3. also apply to external controllers that are not Group Companies.

The enforceability of these provisions must be ensured by internal Group processors by including the following regulation in the agreement for processing on behalf: The data processing activity is subject to the binding corporate rules of the processor, which are considered by the competent supervisory authority to be sufficient to create an adequate level of data protection within the meaning of EU law. In this respect, the binding corporate rules of the processor are binding towards the controller.

8.2. Provisions for Controllers

When issuing the order, the following requirements must be complied with, whereby the department placing the order must ensure that they are met:

» The processor must be chosen based on its ability to cover the required technical and organizational protective measures.

» The contractual standards for data protection provided by the Sales Quality Officer I Officer Corporate Data Protection must be complied with.

» The order must be placed in writing or in electronic form. The instructions on data processing and the responsibilities of the controller and processor must be documented.

Before data processing begins, the controller must confirm by suitable assessment that the processor will fulfill the aforementioned obligations. Provisions established by Garant Group on this subject (such as software tools, instructions on the performance of evaluation, template contracts) must be observed. A processor can document its compliance with data protection requirements in particular by presenting suitable certification. Depending on the risk of data processing, the reviews must be repeated on a regular basis during the term of the contract.

8.3. Provision for internal Processors

The processor can process personal data only as per the controller's instructions.

Processors may engage other Group Companies or third parties (“subcontractors”) to process personal data in their own (sub) contract only with the controller's prior consent. This consent will be granted only if the processor subjects the subcontractor -

contractually or by other comparable legally binding means - to the same data protection obligations to which the processor is subject pursuant to this policy vis-a-vis the Group Company and data subjects.

It must also oblige the subcontractor to take the appropriate technical and organizational protective measures. The form of consent as well as information obligations in the event of changes in the subcontracted relationship must be set out in the contract for services.

Processors are obligated to provide appropriate support to the controller in complying with data protection provisions applicable to the latter, especially by providing all the necessary information. This concerns, in particular, safeguarding » the general principles for processing pursuant to Section 5 » the rights of data subjects pursuant to Section 10 » the notification of data protection incidents pursuant to Section 12 » the provisions for controller and processors pursuant to Section 8 » and the handling of inquiries and investigations by supervisory authorities.

If applicable standards or legal provisions require the processor to carry out the processing contrary to the controller's instructions, or if these provisions prevent the processor from meeting its obligations under this Policy or under the agreement on processing on behalf, then the processor shall immediately inform its controller unless the legal provision in question forbids such notification. This applies accordingly if the processor is unable to comply with the instructions of its controller for other reasons. In such an event, the controller has the right to suspend transmission of the data and/or to terminate the agreement on processing on behalf.

Processors are required to notify their controllers about any legally binding requests from public authorities for disclosure of personal data, unless this is prohibited for other reasons.

At the choice of the controller, processor must delete or return all personal data provided by the controller upon termination of service performance.

Processors are obligated to immediately inform their controller and, if applicable, their controller's client of any asserted claims, requests or complaints from data subjects.

Internal Group controllers also must oblige external processors to comply with the aforementioned regulations.

The specific duties of the processor to the controller are third party beneficiary rights for the data subject.

9 Joint Controllership

In the event that multiple Group Companies jointly define the means and purposes of processing personal data (along with one or more third parties, if applicable) (joint controllers), the companies must conclude an agreement that stipulates their duties and responsibilities to the data subject whose data they process.

The contract templates provided by the Sales Quality Officer I Officer Corporate Data Protection must be observed.

10 Enforceable Rights for Data Subjects

All rights of the data subjects and obligations of the Group companies listed in this section 10 are third party beneficiary rights for the data subject.

The inquiries and complaints submitted in accordance with this Section 10 must generally be answered within one month; in justified exceptions this can be extended to no more than three months after receipt.

10.1 Rights of the Data Subject

A data subject in the EU has the following rights as specified in more detail in EU law vis-à-vis the responsible Group Company or - if the Group Company is the processor - vis-à-vis the controller:

» the right to be informed of the circumstances of the processing of his personal data. The requirements of the Sales Quality Officer I Officer Corporate Data Protection for such information must be observed.

» the right to obtain information about how his data is processed and what rights he is entitled to in this respect. If there are further rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws,

these will remain unaffected. Upon request, the data subject can receive a copy of his personal data (possibly for a reasonable fee), unless interests of third parties worthy of protection prohibit this.

» the right to correct or supplement personal data if they are incorrect or incomplete.

» the right to delete his personal data if he withdraws his consent or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and interests worthy of protection that prohibit deletion must be observed.

» the right to restriction of processing of his data if he disputes its accuracy or if the Group Company no longer needs the data while the data subject needs the data for his legal claims. The data subject can also request that the Group Company restrict the processing of his data if it would otherwise have to delete the data or if it is reviewing an objection by the data subject.

» the right to receive the personal data relating to him, which he has provided on the basis of consent, or in the context of an agreement that was concluded or initiated with him, in a commonly used digital format. He is also entitled to transmit this data to a third party if the data is carried out by automated means and this is technically feasible.

» the right to object to direct marketing at any time. An adequate consent and objection management system must be ensured.

» the right to object to the processing of personal data that is processed on the legal basis of overriding interests of a Group Company or a third party, for reasons relating to his particular personal situation. However, this right of objection does not apply if the Group Company has compelling reasons for processing or if the data is being processed for the establishment, exercise or defense of legal claims. If there is a legitimate objection, the data must be deleted.

In addition, the data subject is also entitled to assert his rights against the Group Company importing the data in a third country.

10.2. Complaints Procedure

Data subjects are entitled to file a complaint with the Sales Quality Officer I Officer Corporate Data Protection if they feel that this Policy has been violated. Complaints of this kind can be submitted by e-mail.

The Group Company established in the EU that exports the data will assist data subjects whose personal data was collected in the EU in establishing the facts and the assertion of their rights under this Policy against the Group Company that imports the data.

In the event that a data subject disagrees with a Group Company's decision on compliance with the requirements (or is otherwise dissatisfied with its handling), he is free to challenge that decision or conduct by exercising his rights. To this end, he may apply to the competent supervisory authority or bring an action in court. Further legal rights and responsibilities shall remain unaffected.

11 Liability & Place of Jurisdiction

11.1. Liability Provisions

The Group company established in the EU (“data exporter”) that initially transferred the personal data to a Group company established in a third country will assume liability for each violation of this Policy by such a third country Group Company that receives data from the EU for third-country processing. This liability includes the obligation to remedy unlawful situations as well as to compensate for material and non-material damage that was caused by a violation of this Policy by Group Companies from third countries.

The data exporter is exempt from some or all of this liability only if it can prove that the third country Group Company that receives data from the EU is not responsible for the action that resulted in damage.

If a Group Company processes personal data as a processor for a company that is not part of the Garant Group and this processing includes the transmission of personal data to subcontractors outside the EU, the Group Company will be liable under this Section 11 for violations of this Data Protection Policy EU and of the agreement to be concluded under Section 8.1. It shall also be liable for the violations of its subcontractor against the foregoing Data Protection Policy EU. In addition, the data subjects affected are entitled to file a claim against the exporting Group Company for reimbursement of the total damage that was caused by the Group Company and the subcontractor. This applies especially if claims by affected data subjects under Section 10 against the controller or its liable legal successor are unenforceable because the latter no longer exists or is insolvent.

Reviewed:
October 2019

This policy will be reviewed on a regular basis to evaluate continued relevance and to monitor compliance.

11.2. Place of Jurisdiction

Any consumer, who is also a data subject, may bring an action before the courts having jurisdiction over him. All other persons may only bring an action before the courts at the seat of the controller.

Any consumer, who is also a data subject, and who claims an infringement of this Policy in the context of a third country processing can assert his legal claims against both the data importing and the data exporting company in the EU. Therefore, the consumer may bring the alleged infringement and the resulting legal claims before the competent courts and regulatory authorities either at the location of the controller or at his habitual residence.

The provisions on liability and place of jurisdiction in this Section are third party beneficiary rights for the data subject.

12 Notification of Data Protection Incidents

In the event of a potential breach of the data security requirements ("data protection incident"), the Group Companies involved have investigation, information and damage mitigation obligations. A data protection incident is a personal data breach if there is a breach of security leading to the unlawful destruction, alteration, unauthorized disclosure or use of personal data. When the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the responsible supervisory authority must generally be informed of the corresponding breach within 72 hours of its initial detection. Furthermore, the data subjects must be notified of any personal data breach likely to result in a high risk to their rights and freedoms. Processors as defined in Section 8.2 are obligated to report data protection incidents immediately to the controller.

If a data protection incident has been identified or suspected within a Group company's area of responsibility, all employees are required to report this immediately in accordance with the Information Security Incident Management Process. Requirements stipulated by Garant Group in this regard (such as software tools, instructions on reporting), must be complied with.

13 Data Protection Organization & Sanctions

13.1 Responsibility

The members of managing bodies of the Group Companies are responsible for data processing in their area of responsibility. Therefore, they are required to ensure that the legal requirements, and those contained in this Data Protection Policy EU, for data protection are met (e.g. national reporting duties). Within their area of responsibility, management staff is responsible for ensuring that organizational, HR and technical measures are in place so that any data processing is carried out in accordance with data protection requirements. Compliance with these requirements is the responsibility of the relevant employees. If public authorities perform data protection checks, the Sales Quality Officer I Officer Corporate Data Protection must be informed immediately.

13.2 Awareness Raising & Training

Management must ensure that its employees receive and attend the required data protection training, including the content and handling of this Policy, if they have constant or frequent access to personal data. The requirements of the Sales Quality Officer I Officer Corporate Data Protection and Data Compliance must be observed.

13.3. Organization

The Sales Quality Officer I Officer Corporate Data Protection is internally independent of instructions regarding the performance of his tasks. He must ensure compliance with national and international data protection laws. He is responsible for this Policy and monitors its compliance. The Sales Quality Officer I Officer Corporate Data Protection is appointed by the Garant Group Board of Management. Generally, Group Companies that are legally obligated to appoint a data protection officer will appoint the Sales Quality Officer I Officer Corporate Data Protection. Specific exceptions have to be agreed upon with the Sales Quality Officer I Officer Corporate Data Protection.

All data subjects can contact the Sales Quality Officer I Officer Corporate Data Protection at any time to express their concerns, ask questions, request information or lodge complaints relating to data protection or data security issues. If requested, concerns and complaints will be handled confidentially.

The contact information of the responsible person is:
Garant Group, Sales Quality Officer I Officer Corporate Data Protection I Pramones str. 8A, LT-94102 Klaipeda, Lithuania
E-Mail: j.dzigajeva@garant.eu

Reviewed:
October 2019

This policy will be reviewed on a regular basis to evaluate continued relevance and to monitor compliance.

The Garant Group has also established a compliance organization, which is described in greater detail in separate internal regulations. The compliance organization supports and supervises the Group Companies in regard to compliance with data protection laws. It defines the content of the data protection training and stipulates the criteria for the group of participants.

13.4. Sanctions

Unlawful processing of personal data or other offenses against data protection law can be prosecuted under regulatory and criminal law in many countries, and can also lead to claims for compensation. Breaches for which individual employees are responsible can lead to disciplinary action under employment law. Violations of this Policy will be penalized in accordance with internal regulations.

13.5. Audit and Controls

Compliance with this Policy and the applicable data protection laws will be reviewed regularly at Group level by way of data protection audits and other checks. The results of these audits must be reported to the Sales Quality Officer I Officer Corporate Data Protection, the responsible Group Company and its data protection officer if one has been appointed. Moreover, the results of this audit must be provided to third-party controllers in accordance with the contractual provisions of the agreement on processing on behalf. Also, third-party controllers are entitled to perform data protection audits on internal data processors according to the contractual provisions of the agreement on processing on behalf. The Group Companies must also perform their own examinations and reviews to determine compliance with this Policy, if so requested by the Sales Quality Officer I Officer Corporate Data Protection.

Garant Group's Supervisory Board must be informed of significant findings as part of existing reporting duties. On request, the results of the reviews will be made available to the competent data protection supervisory authority. The competent data protection supervisory authority can perform its own checks on compliance with the regulations of this Policy, as permitted under national law.

14 Amendments to this Policy and Cooperation with Public Authorities

14.1 Responsibility in the Event of Amendments

The Policy can only be changed by means of the defined procedure for amendment of policies in coordination with the Sales Quality Officer I Officer Corporate Data Protection. Changes that have significant effects on the Policy or affect the level of protection offered by the Policy (i.e. changes to the binding character) must be promptly reported to the competent data protection supervisory authorities, who issue approval of this Policy as binding corporate rules.

The Sales Quality Officer I Officer Corporate Data Protection is responsible for keeping a current list of all Group Companies that are bound by this Policy (further applicable regulation “List of Group Companies bound by the Data Protection Policy EU”). If Group companies process personal data on behalf of non-Group companies, the Group companies will notify these about changes to the list. In the event of changes to the policy affecting the processing conditions, these non-Group companies will be notified in good time so that they are able to object to the amendment or terminate the agreement with the internal processor.

For data subjects outside the Garant Group the latest version of this Policy will be published online at www.garant.eu . This requirement is a third party beneficiary right for the data subject.

If amendments are made to this Policy or the list of affiliated Group Companies, the supervisory authority of the main establishment of Garant Group will be notified of this once a year by the Sales Quality Officer I Officer Corporate Data Protection.

14.2 Cooperation with Authorities

Group Companies that carry out or participate in processing in third countries are obligated to cooperate with the responsible supervisory authorities in matters concerning problems, inquiries or other procedures in connection with the processing of personal data in the context mentioned above. This encompasses the duty to tolerate lawful audits by supervisory authorities. In addition, all lawful instructions from the responsible supervisory authorities based on processing procedures in third countries or provisions of this policy shall be complied with.

If Group Companies are part of an international certification system for binding corporate rules on data protection, they must ensure cooperation with the responsible audit companies and agencies. Participation in such certification systems must be agreed with the Sales Quality Officer I Officer Corporate Data Protection.

The provisions of 14.2 on cooperating with the authorities are third party beneficiary rights for the data subject.

Reviewed:
October 2019

This policy will be reviewed on a regular basis to evaluate continued relevance and to monitor compliance.

14.2. Monitoring and Reporting on the Regulations of Third Countries

The people responsible in third country companies must notify the Sales Quality Officer I Officer Corporate Data Protection immediately if for their company the legitimate expectation exists, that laws or other regulations passed by a country or institution other than the EU and its member states, present the following risks:

» the laws or regulations are such as to prevent the relevant third-country company or other Group Company from meeting its obligations under this Policy when processing data in third countries, or

» the laws or regulations can have serious adverse effects on the rights that data subjects are granted by this Policy for processing in third countries. Especially if the local public authority demands a data transfer that is massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

The Sales Quality Officer I Officer Corporate Data Protection will evaluate the impact and notify the competent data protection authority (if applicable) if the relevant legal requirement is expected to interfere to a significant extent with the guarantees provided by this Policy. This provision is a third party beneficiary right for the data subject.

If a third-country company is required by a public authority to refrain from notifying the data protection supervisory authority about the disclosure of personal data, it shall take all suitable measures to mitigate this prohibition as far as possible or to repeal it, and to provide general information on the requests it received to the competent supervisory authorities.

Garant Group
Pramones 8A, Klaipeda,
Lithuania, EU
www.garant.eu

Reviewed:
October 2019

This policy will be reviewed on a regular basis to evaluate continued relevance and to monitor compliance.