Guideline

Company Guideline Data Protection of Ensus UK Ltd.

Version:	1.0
Valid after:	01.01.2019
Replaced:	
Document:	Company Guideline Data Protection
Responsible:	Grant Pearson

Yarm, 01 January 2019
Ensus UK Limited

The Executive Board

Annual Review:

Subsequently, it is documented by signature that the annual check has taken place and that a change of the instruction is not necessary at present.

Review: (Date, Signature)		Approved (Date, Signature)	

Company Guideline Data Protection of Ensus UK Ltd.

Version 1.0 as of 01.01.2019

Content

1 General information on the data protection guideline

1.1 Objective and relevance

This Data Protection Guideline is the binding basis for legally compliant and sustainable protection of personal data at Ensus UK Ltd. (hereinafter referred to as "Ensus"). The objective of this Guideline is to safeguard and protect the fundamental rights and freedoms of data subjects, in particular their right to the protection of personal data.

Maintaining data protection is the basis for trustful business relationships and Ensus' reputation. Ensus is committed to responsible and legally compliant handling of personal data and strives to protect such data in accordance with the applicable legal provisions.

1.2 Scope of application

This Guideline is binding for all Ensus employees and senior executives, regardless of the nature and scope of their employment. This also applies to external service providers who work for Ensus as part of their commissioning, provided that they process personal data on Ensus' behalf.

The rules and prohibitions of this Guideline apply to any handling of personal data, irrespective of whether in electronic or paper form. Their scope of application also includes all types of data subjects (customers, employees, suppliers, etc.).

2 Legal basis and definitions

The Data Protection Guideline is based on the requirements of the EU General Data Protection Regulation and the UK Data Protection Act. The terms that are essential to the understanding of this Guideline are defined below; further definitions relevant for these regulations are enclosed in Annex 1 to this Guideline.

Personal data means any information relating to an identified or identifiable natural person (data subject). Customer data is just as much a part of personal data as employee personnel data.
For example, the name of a contact person allows as much information to be drawn about a natural person as his or her e-mail address. It is sufficient if the respective information is linked to the name of the person concerned or can be established independently of this from the context. Likewise, a person can be identifiable if the information must first be linked to additional knowledge, e.g. with a license plate number. The manner in which the information arises is irrelevant for its relation to a person. Photos, video or audio recordings can also constitute personal data.

Processing means the performance of any operation or set of operations upon data, whether or not by automatic means, such as collecting, recording, organising, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, dissemination or otherwise making available, the aligning or combining, blocking, erasing or destroying.

3 Permissibility of data processing

The processing of personal data is only permitted if one of the following cases of permission applies. In order to change the defined purpose of the actual data processing, one of the following cases of permission is also required.

Personal data may be processed:

- In the case of an existing contractual relationship with the data subject.
- In the course of pre-contractual measures at the request of the data subject as well as the execution of the contract with the data subject.
- If and to the extent the data subject has consented.
- If there is a legal obligation to which the company is subject.
- If the company has legitimate interests, unless the interests or fundamental rights of the data subject are overriding; this applies in particular to a child. However, data processing based on a legitimate interest should not be carried out without prior legal assessment.

4 Principles for the processing of personal data

4.1 Lawfulness, fairness and transparency

In the processing of personal data, the personal rights of the data subject must be protected. Personal data must be processed in a lawful manner. Transparency regarding the processing of personal data must be ensured vis-à-vis the data subject. When collecting data, the data subject must be informed about the data controller, the purpose of data processing and any data transfer to third parties.

4.2 Purpose limitation

The processing of personal data may only pursue the purposes defined before the collection of the data. Subsequent changes to the purposes are only possible to a limited extent and require either the consent of the data subject or a justification. Data storage without purpose, for example the storage of data in stock for potential future purposes, is not permitted.

4.3 Data minimisation and storage limitation

The data collected must be appropriate to the purpose and limited to the extent necessary for the processing. Before personal data is processed, it must be checked whether and to what extent this is necessary in order to achieve the purpose intended by the processing. If it is possible to achieve the purpose and the effort is proportionate to the intended purpose, anonymised or pseudonymised data must be used.

The principle of storage limitation specifies the principle of data minimisation in terms of time. This includes in particular the achievement of the purpose. The data to which the storage limitation applies are those that enable the identification of the person.

However, data may also lose its relevance for the purpose for which it is processed, e.g. if it is no longer up-to-date.

To ensure that data is not stored for an unnecessarily long time, the stored data must be reviewed at regular intervals. If data are no longer required for the purpose of processing, in accordance with the principle of achievement of purpose they may not be kept in stock for purposes not yet determined.

As a general rule, personal data must be erased in the event of cessation of purpose, unless statutory retention periods prevent such erasure. If this is the case, the data must be kept until the end of this period in such a way that it is accessible only for the smallest possible group of persons. If there is no legal retention period, a three-year retention period is specified, depending on the circumstances. Deviations from this must be justified in writing and checked by the specialist department.

4.4 Accuracy

Personal data must be stored accurately and completely. Necessary adjustments must be made regularly to make the necessary rectifications to keep the data up-to-date. Appropriate measures must be taken to ensure that incomplete or inaccurate data is erased or rectified without delay.

4.5 Integrity and confidentiality

Data secrecy applies to personal data. Processing must ensure the security of personal data through appropriate technical and organisational measures, in particular protection against unauthorised or unlawful processing.

4.6 Other principles (including change of purpose and information obligations)

Data subjects must not be subjected to decisions based solely on automated processing - including profiling - which produces legally binding effects concerning him or her or similarly significantly affects him or her.

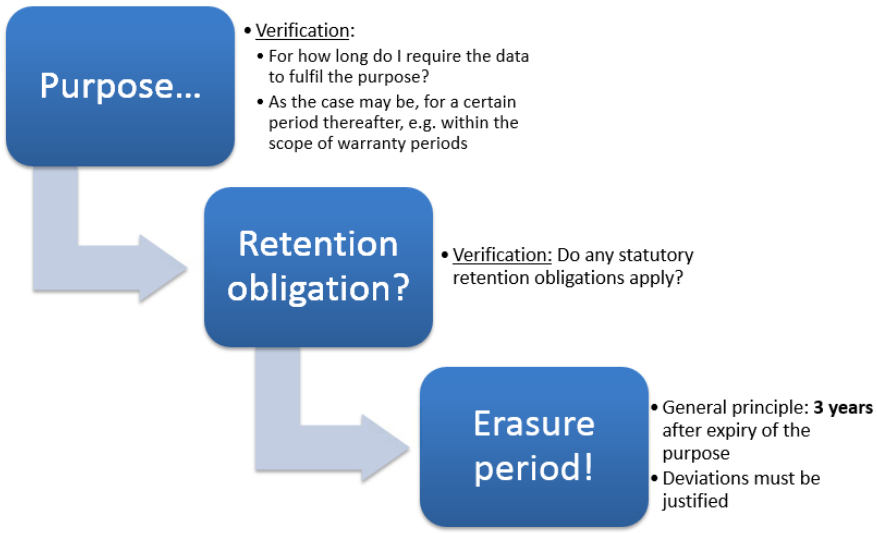
If possible, the use of personal data should be avoided. Pseudonymised or anonymised data processing is preferable.

In addition to the declared consent of the data subject, the modification of a defined objective and purpose on which a data handling was originally based is only permissible if the purpose of further processing is compatible with the original purpose. In particular, the reasonable expectations of the data subject regarding such further processing vis-à-vis the company, the nature of data used, the consequences for the data subject and the possibilities of encryption or pseudonymisation must be taken into account.

When collecting personal data, the data subject must be comprehensively informed about the handling of his/her data. The information must contain the purpose, the identity of the data controller, the recipients of his/her personal data and all other information necessary to ensure fair and transparent processing. The information shall be composed in a comprehensible and easily accessible form and in as simple a language as possible.

If personal data are not collected from the data subject, but are procured, for example, from another company, the data subject must be informed subsequently and comprehensively about the handling of his/her data in accordance with applicable statutory provisions. This applies also to any amendment of a definition of the objective and purpose of data processing.

5 Concept for erasure of data



5.1 General concept for erasure of data

As a general concept for the erasure of data, a three-level process is used that is easy to complete for all responsible persons in business divisions and departments, in which Ensus has imposed on itself a general erasure period of 3 years after expiration of the purpose, unless statutory retention obligations extend this period or special legal requirements (primarily from applicable data protection law) shorten the period. For determination of lawful erasure periods, Ensus shall seek legal / data protection advice.

5.2 Technical implementation of erasure

As soon as the retention period defined by the respective business division or department has expired, the relevant personal data must be erased immediately from all systems and storages. Responsibility for this lies with the respective business division or department, which will receive support in this respect from Central IT Department (ZAO/IT).

6 Special categories of personal data

Special categories of personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data uniquely identifying a natural person, health data or data relating to a natural person's sex life or sexual orientation.

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 statutory permission. Furthermore, additional technical and organisational measures (e.g. encryption during transfer, minimum assignment of rights) must be taken to protect special personal data.

7 Rights of data subjects

The rights that the data subjects may exercise must be observed. Their assertion is to be processed by the responsible department and must not lead to any disadvantages for the data subject.

- Right to information: The data subject may request information as to which personal data about him/her is stored and for what purpose. In cases where personal data is transferred to third parties, information must also be provided to the data subject on the identity of the recipient or on the categories of recipients.
- Rectification: The data subject has the right to have his/her data rectified immediately if they are not accurate.
- Erasure: The data subject is entitled to request the erasure of his/her data if the legal basis for processing the data is lacking or has ceased to exist. The same applies in the event that the purpose of data processing has lapsed due to time or other reasons. Existing retention obligations and legitimate interests that conflict with erasure must be observed.
- Restriction: The data subject has the right to request the restriction of processing if the admissibility no longer exists in whole or in part. (e.g. cessation of purpose)
- Objection: The data subject has the right to object to the processing of his/her data for reasons arising from the special situation of the data subject.
- Right to review automated individual decision-making
- Right to data portability

Data subjects also have the right to lodge a complaint with a supervisory authority regarding a specific data processing.

When processing applications, the identity of the data subject must be established beyond any doubt. If there are reasonable doubts as to the identity of the applicant, additional information may be requested from him/her.
Information shall be provided in writing, unless the data subject has submitted the request for information electronically. The information must be accompanied by a copy of the data of the data subject, which, in addition to the personal data available, also includes the recipients of data, the purpose of storage and all other information required by law in order to make the data subject aware of the processing and assess the lawfulness himself/herself.

The data subject must be informed of all measures taken at his/her request within one month at the latest.

8 Data protection organisation

8.1 General

Ensus is responsible for ensuring an appropriate data protection organisation in order to comply with the requirements of data protection law and this Guideline. The data protection organisation includes the design and implementation of local data protection processes, the provision of appropriate and regular training and the maintenance of the necessary records and documentation.

8.2 Responsibility of the management

Ensus is not legally obligated to appoint an data protection officer. Therefore, the company management is responsible to carry out the following obligations regarding data protection

The company management monitors compliance with applicable data protection laws and other legal data protection requirements, including the requirements of this and other company guidelines on data protection. The company management is responsible for communication with the supervisory authorities. Selected processes are monitored randomly, in a risk-oriented manner for data protection compliance at appropriate intervals.

8.3 List of processing activities

The company has to keep a register of all data processing activities.

8.4 Planning of new data processing and data protection impact assessment

Data protection must be taken into account already at the time of planning new data processing procedures, changes in data processing procedures and the procurement of products and services for data processing, so that risks for data subjects can be identified at an early stage and adequately reduced.

Each business division or department is required to conduct data protection impact assessments for procedures conducted under its responsibility if a high risk to the rights and freedoms of data subjects is to be expected as a result of the data processing. The company management advises the business divisions and departments on the implementation of the data protection impact assessment and on the question of when processing may involve a high risk for data subjects.

8.5 Obligations of employees

Employees are prohibited from collecting, processing or using personal data without authorisation. Any processing carried out by an employee without being assigned to do so within the scope of the performance of his/her duties and without being authorised accordingly is prohibited. Employees may not use personal data for their own private or commercial purposes, transmit it to unauthorised persons or make it available to them in any other way.

Before taking up their activities, they shall undertake to treat personal data confidentially and lawfully. The undertaking is made by the company management using the form provided for this purpose. This obligation survives the termination of the employment relationship. Employees with special confidentiality obligations (e.g. telecommunications secrecy) are also bound by the company management in this respect in writing.

A negligent or even deliberate breach of this Guideline may result in action under employment law, including termination with or without notice. Criminal sanctions and civil law consequences such as damages may also apply.

8.6 Availability, confidentiality and integrity of data

Depending on the nature, scope, circumstances and purposes of data processing and the likelihood of occurrence, a documented assessment of the need for protection and an analysis of the risks to data subjects must be carried out for each procedure.

To ensure the availability, confidentiality and integrity of data, a general security concept is drawn up based on the determination of protection requirements and risk analysis, which is binding for all procedures. This includes the state of the art as well as means and measures for encryption and data backup. The safety concept is to be

regularly reviewed, assessed and evaluated with regard to the effectiveness of the technical and organisational measures provided for therein.

Data processing systems have to be prevented from being used without authorisation. Effective measures to control access to devices must be in place and activated. System accesses must always be blocked in absence.

Employees should only have access to and be able to retrieve personal data if and to the extent necessary for their respective tasks ("need-to-know principle"). This requires the careful division and separation of roles and responsibilities as well as their implementation and maintenance within the framework of authorisation concepts.

Data transmissions via public networks should be encrypted where possible. Encryption is mandatory if the protection of personal data requires it.

Personal data collected for different purposes have to be processed separately. The separation of data must be ensured by suitable technical and organisational measures.

8.7 Behaviour in the event of personal data breaches

Every employee must immediately report violations of this Guideline or statutory requirements of data protection law to his or her supervisor and the company management. The report has to include all relevant information to clarify the facts of the case, in particular the recipient, the persons concerned and the nature and extent of the data transmitted.

Any duty to inform supervisory authorities is to be fulfilled exclusively by the company management. In particular in cases of unlawful transmission of personal data to third parties, unlawful access by third parties to personal data and loss of personal data, the competent supervisory authority must be notified immediately.

The company management must report the violations to the competent data protection authority within 72 hours. Data subjects will be informed by the management. The forwarding and also the obligation to inform are subject to a preliminary examination with regard to the actual risk to the rights of the data subjects. Whether a notification to the competent data protection authority and also information to the data subject is made is subject to the decision of the company management, where necessary with the involvement of external advisors.

8.8 Data protection audits

In order to ensure a high level of data protection, relevant processes may be reviewed by regular audits of internal bodies or by external auditors. The Internal Audit Department (ZAREV) can also be involved in the internal audits. If potential for improvement is identified, immediate remedial measures must be defined and implemented and controls for implementation must be established.

The findings of the audit must be documented. The documentation must be handed over to the company management and the line manager for the respective process.

8.9 Training

Employees who have permanent or regular access to personal data, collect such data or develop systems for processing such data must receive appropriate training on data protection regulations. The company management decides on the form and rotation of the corresponding training courses and supports the creation and continuous further development of training concepts.

8.10 Internal investigations

Measures to clarify the relevant facts and to prevent or detect criminal offences or serious breaches of duty in the employment relationship must be carried out in strict compliance with the relevant statutory data protection regulations. The associated collection and use of data to achieve the purpose of the investigation must be necessary, appropriate and proportionate to the legitimate interests of the data subject.

The data subject shall be informed as soon as possible of the measures taken in relation to him or her.

In all forms of internal investigations, the company management must be involved in advance with regard to the selection and design of any measures.

8.11 Accountability

Compliance with the requirements of this Guideline must be verifiable at all times. Particular attention must be paid in this respect to the traceability and transparency of measures taken, for example by means of associated documentation.

9 Dealing with third parties

9.1 Transfer of data

The transfer of personal data to third parties is only permitted on the basis of a statutory permission or the consent of the data subject.

If the recipient of personal data is located outside the European Union or the European Economic Area, special measures are required to protect the rights and interests of data subjects. Data must not be transmitted if the receiving body does not have an adequate level of data protection or if such level of protection cannot be established, for example, by means of special contractual clauses.

9.2 Internal and external service providers

If (group) internal or external service providers are to have access to personal data, the company management must be informed in advance. Service providers with possible access to personal data must be carefully selected before placing an order. The selection must be documented.

If a service provider is to collect, process or use personal data on behalf of the company, a processing agreement has to be concluded. As the commissioning company, Ensus retains full responsibility for the correct execution of the data processing. Data protection and IT security aspects are to be regulated in the contract for order processing. The Central Purchasing Department (ZAE) is responsible for negotiating and concluding the contract in accordance with its purchasing manual. For these technical and organisational measures, the ZAO/IT must be involved and its assessment of the appropriateness of such measures must be obtained.

The service provider has to be monitored regularly with regard to the technical and organisational measures agreed with it in the contract. The result must be documented.

9.3 Third-party requests for information on data subjects

Should a party request information about data subjects, such as customers or employees of this company, information may only be disclosed if

- the party providing the information can demonstrate a legitimate interest in this respect, and
- a statutory law requires that the information be disclosed, and
- the identity of the person or party making the enquiry has been established beyond any doubt.

10 Entry into force term, updating of the data protection guideline

This Guideline shall enter into force on the date of its signature. The term of the Guideline is not limited.

In the context of the further development of data protection law and technological or organisational changes, this Guideline will be regularly reviewed for any need to adapt or supplement it. This agreement shall continue to apply until the conclusion of a new Data Protection Guideline.

Changes to this Guideline shall be effective without any requirements as to form. The staff and executive employees are to be informed immediately and in an appropriate manner of the changed requirements.

Yarm, 01 January 2019

Ensus UK Ltd.

Annex 1 Definitions

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

Special categories of personal data are information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or a possible trade union membership, as well as genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
A third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Consent can be revoked by the data subject at any time.

Recipient means a natural or legal person, public authority, agency or another body, to which personal data are disclosed, irrespective of whether a third party or not.

Profiling means any form of automated processing of personal data consisting of the use of such personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Controller means the 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.