External

DEKRA
Data Protection Principles

13.09.2024
Version 1.1
DEKRA SE
Group Data Protection

TABLE OF CONTENTS

I. DEKRA's Data Protection Principles

DEKRA is obliged to protect personal data. The fundamental framework for this is provided by the following principles of data protection, which DEKRA must observe in the design and implementation of data processing.

1. Lawfulness and Fairness

When processing personal data, the rights of the data subject must be respected. Personal data must be collected and processed lawfully and fairly. DEKRA processes personal data only if a legal basis exists. This legal basis can result from a law, a contract, prior express consent or a legitimate interest.

2. Transparency

DEKRA shall describe how it collects, processes and stores personal data in a written regional or local data protection notice, if and as required by applicable law. If applicable law gives data subjects certain rights, those rights shall be set forth in the notice. The notice shall be written in a manner that the data subject can comprehend and made publically available (e.g. by posting on the regional website). As a basic rule and if required by applicable law, data subjects must be able to recognise or be informed accordingly about the following, in particular

- identity of the Controller;
- the purpose and legal basis for the data processing;
- the period during which the personal data will be stored;
- the third parties or categories of third parties to whom the data may be disclosed.

3. Purpose limitation

DEKRA shall inform the data subject of (or, if required by applicable law, obtain the consent of the data subject for) the purpose(s) for which his or her data will be processed at or before the time of data collection. DEKRA will not process personal data for a purpose(s) other than those described at the time of data collection, unless the data subject is subsequently informed of (or, if required by applicable law, subsequently provides consent to) the expanded purpose(s) or as otherwise required by applicable law.

4. Data minimisation

DEKRA shall not collect, process or store more personal information than is necessary to accomplish the purpose(s) for which it was collected. If it is possible to achieve the purpose(s) and if the effort involved is proportionate to the intended purpose(s), anonymised, pseudonymised or statistical data shall be used so that the identity of data subjects cannot be determined or can only be determined with disproportionately high effort. Personal data may not be stored for potential future purpose(s) unless this is required or permitted by state law.

5. Storage limitation and data deletion

Personal data that is no longer required after the expiry of legal or business process related retention periods must be securely destroyed or deleted. Personal data may be stored for a longer period of time if the personal data are processed exclusively for archiving purposes in the public interest or for scientific and historical research purposes or for statistical purposes, subject to the implementation of appropriate technical and organizational measures. Instead of destruction or deletion, the data can also be made anonymous.

6. Data quality

DEKRA processes only correct data in its own interest. Irrespective of this, personal data must be correct, complete and - where necessary - up to date. Appropriate measures must be taken to ensure that incorrect, incomplete or outdated personal data are deleted, corrected, supplemented or updated.

7. Data Security – confidentiality, integrity, availability

Data security applies to personal data. They must be treated confidentially and protected by appropriate technical and organizational measures against unauthorised access, unlawful processing or disclosure, as well as accidental loss, alteration or destruction. Taking into account the protection goals of confidentiality, integrity and availability, the Group Information Security Policy valid for DEKRA in its current version applies in this respect.

8. Data Protection by design and by default

As far as possible, DEKRA shall take appropriate technical and organizational measures to ensure that the above principles are adhered to within the framework of any data processing, including through default setting and taking into account the purpose of the processing and by this means in particular ensure that no more data than necessary, no longer than necessary and no more comprehensive than necessary are processed, and access by third parties is restricted as far as possible.

II. Legal basis of data processing

Data processing is only permitted if one of the following legal basis applies. Such legal basis is also required if the purpose of the data processing is to be changed from the original purpose. Details of the data processing purposes must be informed about in data protection policies as part of the relevant contractual documents, terms and conditions and/or the data protection policies available online.

1. Prospect, customer, partner and user data

a. Data processing based on consent

Insofar as data subjects give informed and voluntary consent to DEKRA for the processing of personal data for specific purposes (e.g. passing on of data within the DEKRA Group, evaluation of data for marketing purposes, photographs within the framework of events, newsletters), the permissibility of this data processing is given on this basis. Consent that has been granted can be revoked at any time. The revocation of a consent is only effective for the future and does not affect the lawfulness of the data processed up to the revocation.

Provided that there are no other mandatory formal requirements, declarations of consent must be obtained and administered in writing or electronically (e.g. automated consent management). Under certain circumstances, e.g. in the case of telephone consultation, consent may also be given orally. The granting of such consent must be documented.

b. Data processing necessary for the performance of a contract

The processing of prospective customer, customer and partner data may be carried out in order to provide our services or in the context of other cooperation with third parties for the performance of our corresponding contracts with customers and partners. Personal data of the interested party, customer or partner concerned may be processed for the purpose of entering into, performing and terminating a contract. Entering into contracts also includes the performance of pre-contractual measures which are carried out at the request of an interested party (e.g. preparation of offers, preparation of purchase applications or to fulfil other wishes of an interested party aimed at the conclusion of a contract). The purposes of the data processing are primarily based on our concrete service (e.g. general inspection, preparation of expert opinions, execution of audits, training or consulting) as well as the subject of the cooperation with a partner.

c. Data processing for marketing purposes

If data subjects contact DEKRA with a request for information (e.g. a request for the sending of information material on a service), data processing is permissible for the fulfilment of this request.

Customer loyalty or advertising measures require further legal requirements if required under applicable law. The processing of personal data for the purpose of advertising or market and opinion research is permitted, provided that this is compatible with the purpose for which the data was originally collected. The data subjects must be informed about the use of their data for advertising purposes when the data is collected, as well as in the moment of any use of the data for advertising purposes. If data is collected exclusively for advertising purposes, the provision of such data by the data subject is voluntary. Data subjects shall be informed about the voluntary nature of providing data for these purposes. In the context of communication with the data subjects and to the extent legally required, consent shall be obtained from the data subjects to the

processing of their data for advertising purposes. Data subjects shall be able to choose between the available contact channels such as mail, electronic mail and telephone.

If the data subject objects to the use of his or her data for advertising purposes, further use of his or her data for these purposes is not permitted and they must be blocked for these purposes. Furthermore, existing restrictions of some countries regarding the use of data for advertising purposes must be observed.

d. Data processing due to legal requirements or in the public interest

The processing of personal data is lawful if the processing is necessary to fulfil a legal obligation to which DEKRA is subject. DEKRA is subject to various legal obligations, i.e. legal requirements (e.g. to combat money laundering, financing of terrorism and other criminal acts or to comply with tax laws). The purposes of processing include, among other things, occupational safety measures, credit checks, identity checks, fraud and money laundering prevention, the fulfilment of control and reporting obligations under tax law and the assessment and control of risks within the DEKRA Group.

e. Data processing in order to protect vital interests

The protection of vital interests may take precedence over the protection of personal data in emergency situations. In particular in the case of disasters caused by nature or man it may be necessary for DEKRA to process personal data (e.g. for humanitarian purposes including the monitoring of epidemics or pandemics and their spread). The purpose and scope in these cases are determined by the specific event.

f. Data processing based on legitimate interest

Unless otherwise prohibited by applicable law, personal data may also be processed if this is necessary to pursue a legitimate interest of DEKRA or a third party. Personal data may not be processed on the basis of a legitimate interest if there is an indication in the individual case that the interests of the persons concerned that are worthy of protection outweigh DEKRA's interest in processing. The interests worthy of protection must be examined by the Processing Owner for each processing operation and the result of this weighing of interests must always be documented in accordance with the specifications of the competent data protection supervisory authorities.

g. Data processing of sensitive personal data

Sensitive personal data are data in particular revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or the genetics, biometrics, health or sex life of the data subject. Other data categories may be classified as sensitive personal data or the content of the data categories may be filled in differently, as required by applicable law.

As a matter of principle, sensitive personal data may only be processed as permitted by

law or if the persons concerned have otherwise granted their express consent.

Consent is not required if the processing of personal data requiring special protection is necessary to protect the vital interests of the data subjects or another natural person and the data subjects are not in a position to give their consent for physical or legal reasons. The processing of such data is also permissible if it is absolutely necessary in order to assert, exercise or defend legal claims against the data subject or if data subjects have manifestly made their corresponding data public. The processing of such data is also permissible if this is required for the purpose of health care or other medical necessities.

Such processing is also permitted where necessary to protect against serious cross-border threats to health or to ensure high standards of quality and safety of healthcare.

If the processing of sensitive personal data is planned, the competent contact person from the international data protection organization must be informed in advance.

h. Automated individual decision

DEKRA does not currently use a fully automated decision-making process to establish and conduct business relations. Insofar as such a procedure is necessary in individual cases for the conclusion or performance of a contract or is used based on the consent of the data subjects or on other legal permission, the data subjects must be informed separately of their rights in this respect, insofar as this is required by law. Before introducing automated decision-making, DEKRA consults the responsible contact person at the international data protection organization.

Automated data processing by which individual personality attributes (e.g. creditworthiness) are assessed must not be the exclusive basis for decisions with negative legal consequences or significant impairments for the data subjects. The data subject must be informed of the fact and the result of an automated individual decision and given the opportunity to comment. In order to avoid wrong decisions, a control and a plausibility check by an employee must be guaranteed.

i. User data and internet

If personal data is collected, processed and used on websites or in applications, the data subject must be informed of this in data protection notices and, if applicable, cookie notices. These notices must be integrated in such a way that they are easily recognizable, directly accessible and constantly available to the data subjects. If user profiles are created ("tracking") to evaluate the usage behavior of websites and apps, the affected parties must be informed of this as required by applicable law. Personal tracking may only be carried out if this is permitted by applicable law or if the data subject has given his or her consent. If tracking is carried out under a pseudonym, the data subject should be given the opportunity to object ("opt-out") in the data protection information. If access to personal data is made possible on websites or applications in an area requiring

registration, the identification and authentication of the data subjects must be designed in such a way that adequate protection is achieved for the respective access.

2. Employee data

a. Data processing based on consent

Employee data shall be processed on the basis of an informed consent of the data subject. Declarations of consent must be given voluntarily. Involuntary consents are invalid. In the case of voluntary disclosure of data by the data subject, consent can be assumed if applicable law does not require explicit consent. Consent that has been given can be revoked at any time. The revocation of a consent is only effective for the future and does not affect the lawfulness of the data processed until revocation.

If required by applicable law, declarations of consent must be obtained and administered in writing or electronically (e.g. automated consent management).

b. Data processing necessary for the performance of the employment contract

For the purpose of the employment contract, personal data necessary for the establishment, performance and termination of the employment contract may be processed. Personal data of applicants may be processed when an employment contract is being established. After rejection, the data of applicants must be deleted, taking into account legal deadlines, unless the applicant has consented to further storage for a later selection process. Consent is also required if the data is to be used for further application procedures or before the application is passed on to other Group companies.

In the existing employment contract, data processing must always be related to the purpose of the employment contract, unless one of the following permissions for data processing applies.

If, during the establishment of the employment contract or in the existing employment contract, it is necessary to collect further information about the applicant from a third party, the respective applicable requirements must be taken into account. In case of doubt, the consent of the person concerned must be obtained.

c. Data processing due to legal requirements or in the public interest

The processing of personal employee data is also permitted if applicable legal regulations require, presuppose or permit data processing. The type and scope of data processing must be necessary for the legally permissible data processing and is based on these legal provisions. The interests of the employee worthy of protection must be taken into account.

d. Collective Agreements

If a data processing goes beyond the purpose of the contract, it is also permissible if it is permitted by a Collective Agreement. "Collective Agreements" are in particular agreements between an employer and employee representatives within the scope of the possibilities of the respective labour law. The regulations must extend to the concrete purpose of the desired processing and can be designed within the framework of state data protection law.

Insofar as a Collective Agreement serves as a legal basis within the meaning of data protection law, this must be stated in this collective regulation itself. In addition, appropriate and special measures to safeguard human dignity and the legitimate interests and fundamental rights of employees must be agreed. This concerns, for example, agreements on the transparency of processing, on the transfer of data to affiliated companies, if applicable, or on the permissibility and limits of monitoring employees. If a collective regulation contains specific rules on data processing, the controller shall note this in the data processing record. All employees shall observe the provisions of the applicable Collective Agreements when processing personal data. The Processing Owner brings the specific requirements to the attention of the employees and implements and documents the necessary processes.

e. Data processing in order to protect vital interests

The protection of vital interests may take precedence over the protection of personal data in emergency situations, including in employment relationships. For example, if, in the event of an industrial accident, the data of an employee who is no longer able to act must be transferred to the emergency doctor or hospital for treatment, the processing of personal data by DEKRA may be necessary. In such cases, the purpose and scope are determined by the specific event.

f. Data processing based on legitimate interest

Personal employee data may also be processed if this is necessary to pursue a legitimate interest of DEKRA. As a rule, legitimate interests are justified legally (e.g. the assertion, exercise or defence of legal claims) or economically (e.g. valuation of companies).

Personal data may not be processed on the basis of a legitimate interest if there is an indication in individual cases that the interests of the employee worthy of protection outweigh the interest of DEKRA in processing the data. The existence of interests worthy of protection must be examined by the Processing Owner for each of such processing operation.

Control measures that require the processing of employee data may only be carried out if there is a legal obligation to do so or if there is a justified reason for doing so. The proportionality of the control measure must also be examined if there is a justified reason. The legitimate interests of DEKRA in the implementation of the control measure (e.g.

compliance with legal provisions and internal company rules) must be weighed against a possible interest worthy of protection of the employee affected by the measure in the exclusion of the measure and may only be implemented if they are appropriate. The legitimate interest of DEKRA and the possible interests of the employees worthy of protection must be established and documented prior to each measure. In addition, any further requirements that may exist under state law (e.g. co-determination rights of employee representatives and information rights of those affected) must be taken into account.

g. Data processing of sensitive personal data

Sensitive personal data are data in particular revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or the genetics, biometrics, health or sex life of the data subject. Other data categories may be classified as sensitive personal data or the content of the data categories may be filled in differently, as required by applicable law.

As a matter of principle, sensitive personal data may only be processed if this is permitted by law or if the persons concerned have granted their express consent.

Consent shall not be required where processing of sensitive personal data is necessary to protect the vital interests of the data subject or of another natural person and the data subject is physically or legally incapable of giving consent. The processing of such data is also permissible if it is absolutely necessary in order to assert, exercise or defend legal claims against the data subject or if data subjects have manifestly made their corresponding data public. The processing of such data is also permissible if it is required for the purpose of health care or other medical necessities (e.g. assessment of work capacity).

In addition, processing of sensitive personal data may be permitted if it is necessary to enable DEKRA to comply with existing rights and obligations in the field of labour law. Data relating to criminal offences can often only be processed under special conditions prescribed by national law.

Finally, such processing is allowed where necessary to protect against serious cross-border threats to health or to ensure high standards of quality and safety of healthcare.

If the processing of sensitive personal data is planned, the responsible contact person from the international data protection organization must be informed in advance.

h. Automated individual decision

DEKRA does not currently use a fully automated decision-making process to establish and implement employment relationships. Insofar as personal data are processed automatically in the employment relationship, by means of which individual personality attributes are evaluated (e.g. within the framework of personnel selection or the evaluation of ability profiles), such automated processing must not be the exclusive basis for decisions with negative consequences or significant impairments for the employees

concerned. To avoid wrong decisions, automated procedures must ensure that a natural person evaluates the content of the facts and that this evaluation is the basis for the decision. The employee concerned must also be informed of the fact and the result of an automated individual decision and given the opportunity to comment.

i. Telecommunication and internet

Telephone systems, e-mail addresses, intranet and internet as well as internal social networks are primarily provided by DEKRA as a working tool within the scope of its operational tasks. They may be used within the framework of the respectively applicable legal provisions, Collective Agreements and DEKRA policies.

In the case of permitted use for private purposes, the secrecy of telecommunications and the applicable national telecommunications law must be observed, insofar as these are applicable.

To defend against attacks on the IT infrastructure or on individual users, protective measures can be implemented at the transitions to the DEKRA network which block technically damaging content or analyze the patterns of attacks.

For security reasons, the use of the telephone systems, e-mail addresses, intranet and internet as well as internal social networks can be temporarily logged. Such logging is also carried out if it is required by the applicable data protection law (e.g. for input and access control).

Personal analyses of this data may only be carried out if there is a concrete, well-founded suspicion of a violation of laws or DEKRA policies. These checks may only be carried out by investigating departments in accordance with the principle of proportionality. The applicable laws must be observed as well as the existing group regulations (such as agreements with the works council).

III. Comissioned data processing

A commissioned data processing constellation shall be deemed to exist if a contractor is commissioned by DEKRA or DEKRA by a customer to process personal data, without responsibility for the associated business process being carried out. In such cases, an agreement on commissioned data processing must be concluded - if required by law - both with external contractors and between companies within DEKRA.

In doing so, the commissioning party retains full responsibility for the correct implementation and the permissibility of the data processing. The contractor may only process personal data within the scope of the instructions of the commissioning party. When placing the order, the following instructions must be observed; the Processing Owner must ensure their implementation.

1. The contractor shall be selected according to its suitability for guaranteeing the

necessary technical and organizational protective measures, with the involvement of the responsible contact person of DEKRA's information security organization. A contractor can prove compliance with the requirements of data security by presenting suitable certification or by otherwise satisfying applicable information security requirements.

2. The order must be placed in written form. The instructions for data processing and the responsibilities of the client and the contractor must be documented.
3. The contractual templates provided by Group Data Protection must be observed in principle. This shall not apply if this cannot be achieved vis-à-vis a contractor and the latter has its own contractual standards that take appropriate account of the legal requirements. In this case and in the case of changes to the contractual standards provided by DEKRA that are desired by a contractor, the responsible contact person of DEKRA's international data protection organization must be consulted.

DEKRA shall audit the contractor’s information security practices at reasonable intervals throughout the term of the agreement, taking into account the nature and sensitivity of the personal information that is the subject of the data processing.

IV. Joint Controllership

If two or more DEKRA Group companies or a DEKRA Group company and a third party jointly decide on the purposes and means of processing personal data, such data processing shall be carried out under joint responsibility.

For each case of such jointly controlled data processing, the DEKRA Group companies involved shall transparently define their respective obligations and role with regard to such data processing. The definition must duly reflect the respective actual functions and relationships of the jointly responsible parties vis-à-vis the data subjects. The aim of this specification is to protect the rights and freedoms of the data subjects and to assign responsibility and liability, also with regard to the monitoring and other measures of the supervisory authorities. Where provided by law, an agreement on data processing under joint responsibility must be concluded.

V. Data security

Personal data must be protected at all times against unauthorized access, unlawful processing, disclosure, transmission or disclosure and against loss, falsification or destruction. This applies regardless of whether the data processing is carried out electronically or in paper form. Technical and organizational measures for the protection of personal data must be defined and implemented before the introduction of new data processing procedures, in particular new IT systems. These measures must be based on the state of the art (meaning not the latest technical developments and advances, but the technologies available on the market), the risks posed by the processing and the need for protection of the data. The risks must take into account the severity of the potential damage to

those affected and the probability of occurrence. Furthermore, the implementation costs must not be disproportionate to the identified risks. The person responsible for processing shall in particular consult the responsible contact person from DEKRA's information security organization. The technical and organizational measures for the protection of personal data are part of the Group-wide information security management and must be continuously adapted to technical developments and organizational changes. Their effectiveness must be regularly checked by the Processing Owner with the involvement of the information security organization.

VI. Incident Reporting

DEKRA shall document violations of the protection goals of confidentiality, integrity and availability in the handling of personal data ("**Data Security Incident**") and, in certain cases, shall report these to the data protection supervisory authorities within the legally prescribed reporting deadlines and, if necessary, to notify the persons concerned. Whether or not such a reporting or notification obligation exists must be examined for the following three types of data security incidents:

- **breach of confidentiality –** unauthorized/unintentional publication, access or disclosure
- **breach of integrity –** unauthorized/unintentional change
- **availability breach –** unauthorized/unintentional access prevention or loss

DEKRA must therefore ensure by means of an appropriately designed Incident Report Management that, as soon as a Data Security Incident comes to its attention, the relevant contact person of the information security organization and the data protection organization is informed immediately, so that the existence of any duty to report can be checked and fulfilled in good time.

Any actual or suspected Data Security Incident must then be reported as soon as possible.

DEKRA SE

Group Data Protection
Handwerkstraße 15
70565 Stuttgart
Telefon +49.711.7861-0
konzerndatenschutz@dekra.com