Privacy Policy

Holiday Inn Express Lucerne-Kriens

Table of contents

1. Purpose and basics

This data protection policy contains regulations for the protection of personal data that apply to the Holiday Inn Express Luzern-Kriens. The instructions provide employees with the most important basics of data protection and, together with other measures and documents, enable them to carry out their activities in accordance with the applicable data protection regulations.

Since the company offers hotel-related services and possibly other services and goods and processes and exchanges personal data in this context, Swiss data protection laws and possibly other data protection regulations (e.g. European ones) are relevant for the company.

2. scope

This data protection policy applies to all employees of the company who process personal data. As part of their employment relationship, employees are obliged to comply with the relevant data protection regulations and these data protection instructions.

3. Object

The subject of this data protection policy is the processing of personal data, regardless of the type and form of processing (i.e. on paper, digital, oral, whole, partial or non-automated).

4. Terms

The applicable data protection law defines some important terms. In principle, the following terms have the same meaning as they are defined in the Federal Data Protection Act (DSG). The most important terms have the following meaning:

Personal data: Personal data is all information that relates to a specific or identifiable natural person.

Examples:*Name, address, location data, online identifiers such as device ID, cookie ID, IP address, RFID tags, etc.*

Note: These are natural persons and not legal entities or other entities. But: Information about a contact person of a supplier or another B2B relationship is also considered personal data.

Particularly sensitive personal data: Personal data in the following categories:

- data about religious, philosophical, political or trade union views or activities;
- Data about health, privacy or racial or ethnic affiliation;
- genetic data;
- biometric data that uniquely identifies a natural person;
- data on administrative and criminal prosecutions or sanctions;

- Data on social assistance measures.

Examples:*Recordings from video surveillance systems, data on employee health, employee criminal records, etc.*

Affected person: Any natural person about whom personal data is processed.

Examples:*Guests, employees, partners, suppliers, etc.*

Edit/Process: The processing of personal data includes all handling of personal data, regardless of the means and procedures used.

Examples:*obtaining, storing, retaining, using, modifying, disclosing, archiving, deleting or destroying data.*

5. Principles for processing personal data

The company and all employees observe the following principles when processing personal data:

5.1 Legality, processing in good faith, transparency

Personal data must be processed lawfully, fairly and in a manner that is understandable to the data subject. “Traceability” requires in particular that the procurement of personal data as well as the scope and purpose of the processing is transparent for the data subject (e.g. through a data protection declaration with the necessary information about the respective processing). Whenever personal data is handled, employees must therefore check whether the persons concerned are aware of this and the other information in accordance with section.7/8were informed.

5.2 Earmarking

Personal data must be collected for specified, explicit and legitimate purposes and may be further processed for these purposes. The processing of data for which no purpose is specified, for example in a data protection declaration, is therefore not permitted. If data is to be further processed for a purpose other than that specified, employees must check whether this purpose is still covered by the original purpose.

Under certain circumstances, personal data may be processed for additional purposes that go beyond the original processing purpose at the time the data was collected. In order to determine whether the processing is compatible with a purpose other than the original one, the Company considers, among other things:

- any connection between the purposes for which the personal data were collected and the purposes of the intended further processing;

- the context in which the personal data was collected, in particular with regard to the relationship between the data subjects and the person responsible;

- the type of personal data, in particular whether particularly sensitive personal data is being processed;

- the possible consequences of the intended further processing for the data subjects;

- the existence of appropriate safeguards, which may include encryption or pseudonymization.

5.3 Data minimization

Personal data must be adequate, relevant and limited to the specified purpose. Therefore, no more data may be collected than is necessary for the processing purpose.

5.4 Accuracy of personal data

Personal data must be factually correct and up to date. However, there is no active obligation to investigate the accuracy of the data. However, if there are reasonable indications that personal data is no longer up to date, this suspicion must be investigated and the data concerned must be corrected if necessary.

5.5 Memory limitation

Personal data must be stored in a form that allows the identification of data subjects only for as long as is necessary for the purposes for which they are processed. Data that is no longer needed must therefore be deleted or anonymized. The question of the period after which data is no longer required cannot be generalized and must be specified in area-specific instructions or assessed on a case-by-case basis. The company and all employees of the company do not store personal data longer than is necessary for the purposes for which it was originally collected or later processed.

5.6 Integrity and confidentiality (“data security”)

Personal data must be processed in a manner that ensures appropriate security of the personal data. They must therefore be protected by appropriate technical and organizational measures against unauthorized or unlawful processing and against accidental loss, accidental destruction or accidental damage. In particular, employees must ensure that other people, including other employees, cannot access or edit personal data unless their authorization is clearly established.

5.7 Documentation requirement

The company management or the hotel management ensures that the principles mentioned are adhered to for all personal data. You can provide documented evidence of compliance at any time.

5.8 Consents

The company obtains the necessary consent from the data subjects in a timely manner, i.e. before any processing for which consent is required is carried out.

If consent must be given expressly, consent is given through a clear confirmatory act which voluntarily, for the specific case, expresses in an informed and unambiguous manner that the data subject agrees to the processing of the personal data relating to him or her.

A consent form is provided in an understandable and easily accessible form and in clear, simple language. It is clearly distinguishable from other matters and does not contain any unfair terms.

In addition, the data subject is provided with a simple method with which they can revoke their consent at any time.

6. Special processing activities

6.1 Processing of particularly sensitive personal data

Particularly sensitive personal data will not be processed. The company and all employees process special personal data requiring protection only after consultation with the data protection coordination office, under the following conditions and only to the extent that the processing does not conflict with any legal regulations:

- The data subject has expressly consented to the processing of the data for one or more specified purposes;

- the processing is necessary to enable the company or the data subject to exercise their rights under labor law and social security and social protection law and to fulfill their obligations in this regard;

- the processing relates to personal data that the data subject has obviously made public;

- Processing is necessary to assert, exercise or defend legal claims or in the event of court action.

The employees note that such data is particularly sensitive information and do not process it until the data protection coordination office has confirmed its legality.

6.2 Processing of a child's personal data

Personal data of a child will generally only be processed if the child has reached the age of sixteen. If the child has not yet reached the age of sixteen, their personal data will only be processed if and to the extent that consent to the processing is given by the child's legal representative.

In such cases, the company and all employees make reasonable efforts to ensure that consent has been given by the child's legal representative.

6.3 Digital Marketing

No communications for advertising or marketing purposes will be sent to contacts via digital media such as mobile phones, email or the Internet without first obtaining the consent of the data subjects. If consent has been given to the processing of personal data for digital marketing purposes, the data subject will be informed in any communication that they have the right to withdraw their consent at any time.

6.4 Directory of processing activities

The company and, if applicable, its representatives keep a record of all processing activities under its responsibility. This contains at least the following information:

- The identity of the controller, i.e. the name and contact details of the company and, if applicable, those jointly responsible with it, their representative, if applicable, and the data protection officer, if applicable;

- the purposes of the processing;

- a description of the categories of data subjects and the categories of personal data processed;

- the categories of recipients to whom the personal data have been or will be disclosed (including recipients in third countries or international organizations);

- if possible, the retention period of the personal data or the criteria for determining that period;

- if possible, a general description of the technical and organizational measures;

- if the data is disclosed abroad, the indication of the country and the guarantees implemented to ensure an adequate level of data protection.

7. Obligations to provide information when collecting personal data directly from the data subject

At the time the personal data is collected, the company must provide the data subjects with the following information in particular:

- identity and contact details;
- the processing purpose(s);
- if applicable, the recipients or categories of recipients of the personal data;
- if the personal data is disclosed abroad: the State or the international body and, if necessary, the guarantees to ensure an adequate level of data protection or the application of an exception to ensure an adequate level of data protection;
- When making so-called automated individual decisions: About the decision, which is made without human influence, the opportunity for the person concerned to express their point of view and the opportunity for the automated individual decision to be reviewed by a natural person.

If necessary, the applicable data protection law may provide for additional content, such as European data protection law, which additionally stipulates that the following information must be included in the information:

- the legal basis for the processing;
- where applicable, the intention to transfer the personal data to a third country and the presence or absence of an adequacy decision by the EU Commission, a reference to the appropriate or appropriate safeguards and the possibility of obtaining a copy of them or where they are available are.
- the period for which the personal data will be stored or, if this is not possible, the criteria for determining that period;
- the existence of a right to information about the personal data concerned and to rectification or deletion or to restriction of processing or a right to object to processing and the right to data portability;
- if applicable, the existence of a right to withdraw consent at any time without affecting the lawfulness of the processing carried out based on the consent before its withdrawal;
- the existence of a right to lodge a complaint with a supervisory authority;

- the existence of automated decision-making including profiling and - at least in these cases - meaningful information about the logic involved as well as the scope and intended effects of such processing for the data subject.

This information is made available to the data subjects, for example via a data protection declaration.

8. Information obligations when collecting personal data indirectly

Personal data about data subjects can also be collected indirectly, i.e. from third parties. However, this does not release the company from informing the person concerned about the processing. In addition to those under paragraph7listed information, the company informs the data subject of the categories of personal data processed. The information must be communicated to the data subject no later than one month after the company received the personal data from the third party or at the latest at the time of disclosure to a third party.

If necessary, the applicable data protection law may provide for additional content, such as European data protection law, which additionally stipulates that the following information must be included in the information (in addition to section7above):

- what source the personal data comes from and, if applicable, whether it comes from publicly available sources.

9. Rights of data subjects

The company and all employees observe the following rights of the data subjects:

9.1 right of providing information

Any data subject whose personal data the Company processes has the right to request confirmation from the Company as to whether personal data relating to the requesting data subject is being processed. To do this, the data subject must submit a written request via email to the office responsible for data protection at the company. Before answering the request, the identity of the person concerned must be verified.

If the identity has been established beyond doubt, the data subject has the right to receive the following information regarding their own personal data:

- the identity and contact details of the person responsible;

- the processed personal data as such;

- the processing purposes;

- the retention period of the personal data or, if this is not possible, the criteria for determining that retention period;

- the available information about the origin of the personal data, insofar as it was not obtained from the data subject;

- if applicable, the existence of an automated individual decision and the logic on which the decision is based;

- where appropriate, the recipients or categories of recipients to whom personal data are disclosed and the State or international body and, where appropriate, the safeguards to ensure an adequate level of data protection or the application of an exception to ensure an adequate level of data protection.

If necessary, the applicable data protection law may provide for additional content, such as European data protection law, which additionally stipulates that the following information must be communicated to the data subject:

- the existence of a right to rectification or deletion of personal data concerning you or to restriction of processing by the controller or a right to object to such processing;

- the existence of a right to lodge a complaint with a supervisory authority;

- the existence of automated decision-making, including profiling, and - at least in these cases - meaningful information about the logic involved and the intended effects of such processing for the data subject.

The company provides a copy of the personal data that is the subject of processing.

By passing on the requested information to the data subject, personal data of another data subject could, under certain circumstances, be disclosed. In such cases, the information in question must be redacted or withheld as deemed necessary or appropriate to protect that person's rights.

9.2 Right to rectification

The data subject has the right to immediately request that the company correct any inaccurate personal data concerning them. Taking into account the purposes of the processing, the data subject has the right to request that incomplete personal data be completed, including by means of a supplementary statement.

9.3 Right to deletion (“right to be forgotten”)

The data subject has the right, under certain conditions, to request that the company delete personal data concerning him or her immediately, and the company is obliged to delete personal data immediately.

9.4 Right to restrict processing

The data subject has the right to request that processing be restricted if one of the following conditions is met:

- the accuracy of the personal data is disputed by the person concerned (including entry of a dispute note). The processing is restricted for a period that allows the person responsible to check the accuracy of the personal data;

- the processing is unlawful and the data subject refuses the deletion of the personal data and instead requests the restriction of the use of the personal data;

- the company no longer needs the personal data for the purposes of processing. However, the data subject needs it to assert, exercise or defend legal claims;

- the data subject has lodged an objection to the processing in accordance with the right to object. The restriction takes place as long as it is not yet clear whether the company's legitimate reasons outweigh those of the data subject.

If processing has been restricted, this personal data - apart from its storage - may only be processed with the consent of the person concerned, to assert, exercise or defend legal claims, to protect the rights of another natural or legal person or for reasons of important public interest .

A data subject who has obtained a restriction on processing will be informed by the person responsible before the restriction is lifted.

9.5 Data portability (“data portability”)

The data subject has the right to receive the personal data concerning him or her that he or she has provided to the company in a structured, commonly used and machine-readable format. You also have the right to transmit this data to another company without hindrance, provided that:

- Processing is based on the consent of the data subject;

- processing is processed in direct connection with the conclusion or execution of a contract between the company and the data subject; or

- processing is carried out using automated procedures.

9.6 Right to object

The data subject has the right to object at any time to the processing of personal data concerning them for reasons arising from their particular situation.

In such cases, the company will no longer process the personal data unless it can demonstrate compelling legitimate reasons for the processing that outweigh the interests, rights and freedoms of the data subject, or the processing serves to assert, exercise or defend legal claims.

9.7 Rights for automated individual decisions

The data subject has the right that decisions that have legal effects on him or her or that significantly affect him in a similar way are not based exclusively on automated processing. Exceptions are permitted as long as they are provided for by law.

The company only uses automated individual decisions that have legal effects against it if the decision is necessary for the conclusion or performance of a contract between the data subject and the company, is necessary due to applicable legal regulations or with the express consent of the data subject Person.

Decisions in this sense are those that are based on purely automated data processing and either have legal effects on the data subject or similarly significantly affect the data subject. For example, in the case of an automated credit check, on the basis of which a contract with a person may be rejected, the requirements of this section must be observed.

Profiling is any type of automated processing of personal data that involves using this personal data to evaluate certain personal aspects relating to a natural person, in particular aspects relating to work performance, economic situation, health, personal preferences, Analyze or predict the interests, reliability, behavior, location or movements of that natural person. If profiling is combined with an automated individual decision, which either has legal effect on the data subject or similarly significantly affects the data subject, the provisions of this section must also be observed.

The company ensures that profiling and automated individual decisions are based on correct data in individual cases.

9.8 Procedure for requests from affected persons

10. Transmission of personal data to third parties

10.1 principle

Any transfer of personal data abroad is only permitted if an adequate level of data protection can be ensured for the third country or international organization in question. A state has an adequate level of data protection if this has been determined by the responsible authority (in Switzerland by the FDPIC or the Federal Council; in the EU by the EU Commission).

If personal data is ever transferred to third countries without an adequacy decision, appropriate safeguards must be put in place. A decision on this is only permissible with the consent of the data protection coordination office.

10.2 Transfers between group companies

All of the company's group companies represent so-called third parties in terms of data protection law. As a basis for a uniform group-wide approach, the companies conclude an intercompany contract, whereby all group companies are used both as the "responsible person" (controller) and as the "processor". The intercompany contract regulates the obligations of the contracting parties according to their role as controller and their role as processor.

10.3 Transfers to other third parties

The company only transfers personal data to third parties and grants third parties access to personal data if it is guaranteed that the data will be processed lawfully and adequately protected by the recipient:

- If the third party is considered the controller, the Company enters into a contract with the controller defining the responsibilities of each party regarding the personal data transmitted.

- If the third party is considered a processor, the company concludes a corresponding order data processing contract with the processor, which obliges the processor to comply with data protection principles. In particular, he is obliged to protect the data from further disclosure, to only process it in accordance with the company's instructions, to implement appropriate technical and organizational measures to protect personal data and to report breaches of data security.

11. Technical and organizational measures

The company takes appropriate technical and organizational measures to ensure the security of personal data in accordance with the applicable data protection regulations. Violations of data security (e.g. in the event of a hacker attack) are reported to the data protection coordination office in accordance with a separate instruction.

12. Data protection through technology design and through data protection-friendly default settings

The company ensures that data protection principles are taken into account at an early stage in new projects and are incorporated into the technical implementation ("Privacy by Design").

The company also takes appropriate technical and organizational measures to ensure that default settings ensure that only personal data that is necessary for the respective processing purpose is processed. In particular, it is ensured that the respective default settings are data protection-friendly (“Privacy by Default”).

13. Data protection impact assessment

The company carries out a preliminary assessment of the consequences of planned processing operations if processing could entail a high risk for the personality or the fundamental rights of the person concerned.

The examination of whether a data protection impact assessment is necessary must be carried out in particular when using new technologies or with new types of data processing operations, as well as on the type, scope, circumstances and purpose of the processing (e.g. in the case of extensive processing of particularly sensitive data or in the systematic and extensive monitoring of public areas [e.g. video surveillance systems]).

The company obtains the advice of the data protection coordination office in advance when carrying out a data protection impact assessment. Data protection impact assessments are carried out in accordance with the separate internal guidelines.

14. Reporting Data Breach

A breach of data security occurs if a breach of security results in personal data being accidentally or unlawfully lost, deleted, destroyed or altered, or disclosed or made accessible to unauthorized persons.

In the event of a breach of data security, the company will report this to the relevant supervisory authority immediately and, if possible, within 72 hours of becoming aware of the breach, as soon as the breach of personal data protection is likely to result in a high risk to the rights and freedoms of natural persons. The company will inform the data subject if it is necessary for their protection or if the responsible supervisory authority requests it.

The process for internally reporting a data security breach is governed by a separate policy.

15. Responsibilities

15.1 Management or the hotel management

The management or the hotel management defines the overarching principles for ensuring data protection in the company. It appoints a person responsible for data protection - the data protection coordination office - who is responsible for enforcing the data protection requirements.

15.2 Superiors

Supervisors at all levels are responsible for enforcing and complying with data protection regulations in their areas of responsibility. In collaboration with the Data Protection Coordination Office, they ensure training and awareness-raising for their employees. They act as role models and promote the motivation of employees to comply with data protection measures.

15.3 The data protection coordination office

The company has appointed a data protection coordination point. The Data Protection Coordination Office is the central contact point for data protection questions and can be contacted via gm@hiex-luzern.ch or telephone 041 545 69 69.

The data protection coordination office has the following tasks in particular:

- You are responsible for the documents for this data protection instruction.
- It supports the company in enforcing and implementing data protection.
- It monitors and takes into account the development of legal requirements in the area of data protection.

The enforcement of this directive is not the responsibility of the data protection coordination office but solely of the superiors.

Further tasks are defined in the data protection coordination office's specifications.

16. Sanctions

Violations of this data protection policy may result in disciplinary measures and/or civil and/or criminal penalties.

17. Final provisions

17.1 Changes and additions

This data protection policy can only be changed, supplemented or canceled in writing by a decision of the management or the hotel management. Any addition, deletion or modification of individual provisions shall be qualified as an amendment or supplement. Corrections of a formal nature are excluded from this.

17.2 Supplementary documents

This data protection policy represents the basis for the company's data protection regulations. Based on this, further documents, instructions and processes can be developed that are necessary in connection with the processing of personal data.

17.3 Access to this policy and changes

This data protection policy is accessible to all employees via the company's existing policy system or via other media as decided by the data protection coordination office.

Changes or additions to this data protection policy come into force at the moment of publication on www.hiex-luzern.ch/datenschutz.

17.4 Come into effect

This data protection policy comes into force on September 1st, 2023.