HIAG

HIAG Group Data Protection Policy

1 May 2024

1. Purpose

HIAG Immobilien Holding AG, Basel, Switzerland (the **"Company"**) has adopted this policy to regulate the handling of personal data of customers and employees of the Company. The term "Company" includes all subsidiaries of the Company in Switzerland. The loss of personal data can result in substantial harm to individuals, including disclosure of sensitive data, inconvenience and fraudulent use of the information. Protecting the confidentiality and integrity of personal data is an important task that must be taken seriously at all times. Compliance with this Data Protection Policy ("Policy") is mandatory. Please note that the rights of individuals may vary depending on the applicable jurisdiction.

The purpose of this Policy is

- to define personal data and sensitive personal data;
- to establish general principles for the protection of personal data;
- to assign responsibility for the protection of personal data;
- to prevent risks under criminal law (in particular, false or incomplete information can result in fines of up to CHF 250,000);
- to define processes and templates for requests for information and data security breaches as well as data protection impact assessments (see in particular **Annexes 1 to 3**).

2. Scope

This Policy applies to all employees of the Company (**"you"**) and agents and representatives who have access to personal data collected or otherwise held by the Company. This Policy applies to all personal data that is collected, managed, transmitted, stored, retained, modified, disclosed, erased, destroyed or otherwise used by the Company, regardless of whether it relates to employees, customers or other natural persons.

3. Definitions

"Order processor" is defined and delimited below under **"Controller"**.

"Processing" means any handling of personal data, regardless of the means and procedures used. The term "processing" is to be interpreted very broadly and refers not only to the digital processing and evaluation of electronic data, but also to physical documents, e.g. paper files. Types of processing include, in particular, the collection, storage, retention,

use, modification, active transmission, passive sharing, archiving, erasure or destruction of personal data.

"Data subject" is an identified or identifiable natural person whose personal data is processed.

"FADP" refers to the Federal Act on Data Protection of 25 September 2020.

"GDPR" refers to the General Data Protection Regulation of the European Union (Regulation (EU) 2016/679).

"DPO" is the Federal Ordinance on Data Protection of 31 August 2022.

"Personal data" is any information relating to an identified or identifiable natural person. An identifiable natural person is someone who can be identified, either directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This information includes, among other things, the following:

- names;
- addresses;
- telephone numbers;
- email addresses;
- employee identification numbers;
- AHV (social insurance) numbers;
- user identification and account access data, passwords, PINs and answers to security questions;
- bank account numbers;
- image and sound recordings;
- technical data (e.g. IP address);
- geolocation data; and
- biometric, medical, health or health insurance information.

"Sensitive personal data" is personal data whose processing is subject to stricter legal requirements than the processing of simple personal data (e.g. address, salary). This qualification stems from the fact that, in the opinion of the legislator, the categories of data designated as sensitive affect the personality of data subjects to such an extent that their

processing always constitutes an infringement of personal rights. Examples of sensitive personal data are

- biometric, medical, health (physical and mental health) or health insurance information;
- religious and ideological beliefs and political opinions;
- trade union membership;
- social insurance benefits relating to illness and accidents;
- membership of a race or ethnic group; and
- criminal record entries.

In most jurisdictions, the law defines the types of information that are subject to increased protection. If you have any questions about whether personal data can be categorised as sensitive personal data, please contact the General Counsel.

"Data security breach" means any act or omission by an internal or external person that compromises the security, confidentiality or integrity of personal data or the physical, technical, administrative or organisational security measures taken by the Company or a third-party service provider to protect personal data. The loss, unintentional or unlawful erasure, destruction, amendment or unauthorised access to personal data and its disclosure to unauthorised persons constitute data security breaches.

"Controller" is the natural person or legal entity who alone or jointly with others determines the purposes and means of processing. This is not the same as the **"order processor"**, who merely processes personal data on behalf of the controller. To differentiate between the two roles:

Order processing applies under the FADP (and also as defined by the GDPR) if

(a) a contractor (i.e. the order processor) on behalf of a client (i.e. the controller) processes personal data;

(b) the contractor may only process the data for the purpose of performing the order (and not for its own purposes);

(c) the contractor processes the data in accordance with the instructions/specifications of the client – without the contractor having a high degree of autonomy in the performance of the order; and

(d) the main focus of the service is data processing (e.g. data hosting in the form of data storage). If the focus of the service does not fall on data processing, no order processing agreement has to be concluded or there is no order processing.

4. Processing of personal data

4.1 Fair and lawful processing

4.1.1 General

Whenever the Company processes personal data, it must ensure that the processing is lawful, fair and transparent towards the data subject.

For certain processing operations, the Company acts as controller or joint controller, and for others as order processor. If the Company acts as controller, it must ensure that it fulfils its obligations under data protection law: most of the obligations under the FADP (and also the GDPR) apply to the controller. The duty to provide information, for example, is central: Data subjects must be informed transparently about the processing of their personal data. In addition, the controller must conclude data processing agreements (often abbreviated to **"DPA"**) with its mandated order processors.

If the Company acts as a processor, it generally processes personal data on behalf of its customers. In these cases, the customer is responsible for complying with the basic obligations of the FADP (or the GDPR, as the case may be). However, the Company must also handle personal data with care in these cases. In particular, all obligations under the DPA concluded with the customer must be observed in order to prevent claims for damages.

4.1.2 Exceptional applicability of GDPR

In principle, the Company is subject to Swiss data protection law when processing data and must therefore comply with the FADP and the DPO. In the EU and the EEA (Norway, Iceland and the Principality of Liechtenstein), however, the GDPR applies. The FADP and DPO are generally more liberal than the GDPR – namely with regard to the obligations to be met and also with regard to the penalties for breaches of duty.

However, Swiss companies must comply with the GDPR in certain cases:

If a Swiss company has a branch (i.e. subsidiary, branch office, branch) in the EU/EEA, (only) this branch must comply with the GDPR.

If services and goods are offered to persons in the EU/EEA, the GDPR must (only) be observed with regard to these foreign customers / end customers.

If tracking tools (e.g. Google Analytics) are used and the behaviour of persons residing in the EU/EEA is observed. Here too, the GDPR only applies to these foreign persons.

And finally, if a Swiss company processes data as an order processor for a company that is subject to the GDPR. The DPA is then also regularly concluded in accordance with the GDPR.

A key distinction between the FADP and the GDPR is the justification and necessary lawful bases:

A lawful basis is required for the *processing of personal data* under the GDPR, but not generally for the *processing of personal data* under the FADP. In contrast to the GDPR, the FADP does not apply any justification for data processing – personal data may be processed as long as the processing principles (see section 4.2 below, e.g. accuracy and purpose limitations) are complied with. Justifications are only relevant under the FADP when it comes to breaches of privacy. However, under the GDPR personal data may only be processed if at least one of the following lawful bases exists, whereby consent also plays a role in certain cases under the FADP if sensitive personal data is processed:

Consent: *Consent is the simplest lawful basis for the processing of personal data. It is important to note that consent must be given voluntarily, specifically, informed and unambiguously. Consent can be given by written or verbal declaration and also by electronic means, e.g. by ticking a box when visiting a website, provided that it is clear that consent to processing is being given. Silence, pre-ticked boxes or inactivity does not constitute consent.*

Whenever companies process ***sensitive*** *personal data – or personal data requiring* ***special protection*** *as per the FADP – the* ***explicit*** *consent of the data subject is required. This always applies under the GDPR, but only applies under the FADP where the FADP defines such exceptional consent as a condition – this is mainly the case for foreign data disclosures and automated individual decisions, but also, for example, if health data is disclosed to third parties.*

Consent can be withdrawn at any time, and withdrawal of consent should be as easy as the granting of consent. The cancellation does not affect the lawfulness of the previous processing.

Contractual necessity: *The processing of personal data is justified if processing is necessary for the performance of a contract to which the data subject is party.*

Compliance with legal obligations: *The Company is authorised to process personal data if processing is necessary to fulfil a legal obligation.*

Vital interests: *Processing is justified if it is necessary to protect the vital interests of the data subject or another person.*

Public task: *Public task refers to processing that is necessary for a specific public interest. Examples include taxes, reporting of an offence or crime, public health, and the quality and safety of products.*

Legitimate interest: *A legitimate interest can be described as an advantage for a company or a group of companies that may result from the processing of personal data. Whenever the Company wishes to use a legitimate interest as the basis for processing, it must ensure that a balance is struck between the Company's interests and the rights and interests of the data subject.*

4.2 Notification and procurement of data, and principle of purpose limitation

It is the Company's policy that if it obtains personal data for a specific purpose, including for personnel or employment purposes, it must inform the data subjects about how it will use, store, disclose, protect and retain this personal data by providing the data subject with a privacy policy or a data protection notice at the time the personal data is collected (principle of transparency; see also section 4.7). You may only collect personal data in accordance with the applicable Company policies, notices and, where the GDPR is applicable, with the consent of the data subject, and the personal data that is collected must be restricted to what is reasonably necessary to meet the Company's legitimate business purposes or where required to comply with the law. The principle of purpose limitation can therefore be summarised as follows: personal data may only be processed for the purpose that was communicated to the data subject when the data was collected or that was apparent to the data subject (legitimate business purposes of the Company).

4.3 Access, use and disclosure of personal data

You may only access personal data if this information relates to your professional duties and is necessary for carrying out your professional duties. You may not access personal data for any reason that is not related to your professional duties. You may not use personal data in a way that is incompatible with the notice provided to the data subject at the time of data collection. If you are unsure whether a particular use or disclosure is appropriate, you should contact the General Counsel. You may only pass on personal data to another employee of the Company if the recipient has a work-related need to know the information. Personal data may only be disclosed to a third-party service provider, agent or representative if they need to know the information in order to provide the contractually agreed services and if the disclosure of the personal data complies with the information on data protection given to the data subject. In this case, it must also be checked whether a DPA has been concluded with the third-party service provider, agent or representative. If this is not the case, the matter must be reported to the General Counsel.

4.4 Correctness

You may only collect, manage and use personal data that is accurate, complete and relevant to the purposes for which it was collected. Incorrect data must be erased or corrected promptly.

4.5 Data security

You are responsible for the protection of personal data in the Company. The Company has adopted an Information Security Policy that defines technical, administrative and physical security measures for the protection of personal data. You must at all times comply with the security procedures set out in the Information Security Policy. You must take special care to protect sensitive personal data from loss, unauthorised access and unauthorised disclosure.

4.6 Principle of reasonableness, data minimisation and erasure

Processing of personal data must be suitable and objectively necessary to achieve a legitimate aim. This means that only as much personal data may be collected and processed as is necessary for meeting the purpose. As soon as the personal data is no longer required, it must be erased or anonymised.

4.7 Transparency and Group Privacy Policy

The Company must be transparent when processing personal data. Transparency refers to the right of the data subject to retain control over their personal data and obliges the Company to implement the measures that are necessary to ensure that the required information is provided to the data subject. The data subject must be provided with the following information when their personal data is collected:

- the identity and contact details of the controller;
- the purposes for processing;
- where applicable, the recipients or categories of recipients to whom personal data is disclosed.

In individual cases, further information may also be required if the following conditions are met:

- If the personal data is not collected from the data subject, the data subject must be informed of the categories of personal data processed.
- If the personal data is disclosed abroad, the data subject must also be informed of the country in question and, if applicable, the protective measures taken.

Ultimately, acting transparently means that the Company has to communicate all information relating to the processing to the data subject and that the Company has to make this information easily accessible and understandable in clear and plain language. The Company must make the data subject aware of the risks, rules, guarantees and rights in connection with the processing. The Company has published a Group Privacy Policy on its website: https://www.hiag.com/en/privacy-policy/. Data subjects do not have to be explicitly informed of this Privacy Policy; however, this may be useful in individual cases (especially if sensitive personal data is processed, at the beginning of a new contractual relationship or when introducing new technical applications [e.g. a mobile app]). The Privacy Policy is one-sided information provided by the Company, can be amended at any time and does not become part of contracts with data subjects. For this reason, data subjects do not have to give their consent to the Group Privacy Policy.

4.8 Rights of data subjects

People have rights when it comes to the handling of their personal data. These rights may vary depending on the applicable jurisdiction, but may include, for example, the following:

4.8.1 Right to information – handling of requests for information

Any person may request information from the controller as to whether personal data relating to them is being processed. Such requests for information are usually made in writing (by the data subject or their lawyer) and in most cases must be answered free of charge, in writing and within 30 days. If a request for information is made verbally, the data subject must be asked to repeat their request in writing. In addition, a copy of the applicant's ID must always be requested (or a power of attorney).

When providing the information, three things are particularly important and must always be taken into account: (i) when providing information, a declaration of completeness must never be given, (ii) if the request for information explicitly or implicitly refers to specific information, only this information and no further information must be provided, and (iii) if the request for information could serve purposes that are not related to data protection or are contrary to data protection, the request for information must not be answered and instead attention must be drawn to this fact. Under no circumstances may the right to information be used to obtain evidence (e.g. in the event of a possible legal dispute) or for a data subject's accounting purposes. Obviously querulous applications or repeated applications must also be rejected.

Further details on the mandatory procedure to be followed and a template for a response letter to requests for information can be found in **Annex 3**.

4.8.2 Right to erasure

In Switzerland, unlike in the EU and the EEA, there is no right to be forgotten. However, a data subject may request the controller to erase their personal data and no longer process it. This request may be made because (i) the processing is no longer necessary for the purpose for which the personal data was collected, or (ii) the data subject has exercised their right to withdraw consent, or (iii) the personal data is being processed unlawfully, or (iv) erasure is required by law.

4.8.3 Right of objection

The data subject has the right to object to direct marketing at any time (e.g. to unsubscribe from the newsletter). In this case, the Company is obliged to stop using the personal data for marketing purposes.

4.8.4 Right to data portability

The data subject may ask the controller to hand over the personal data disclosed by the data subject to the controller and may also ask the controller to transmit their personal data to another controller. The Company must ensure that this is done in a common electronic format, which is only possible for electronically processed data – which is why there is no right to the portability or transmission of personal data if only paper files are available (in individual cases, however, the request may be met if there is no disproportionate effort involved).

4.8.5 Criminal sanctions

You must comply with the applicable laws regarding the rights of data subjects. If you are not sure which legal requirements apply, or if you receive an enquiry or complaint from a data subject regarding the processing of their personal data, please contact the Legal Department immediately. This is particularly important because, for example, requests for information must be answered within 30 days and criminal sanctions may be imposed if incorrect information is provided. In Switzerland, fines of up to CHF 250,000 may be imposed if duties of information, disclosure, co-operation and due diligence are breached. In the EU and EEA, the penalties are stricter and higher fines are possible.

5. Data protection impact assessment

Before introducing a new system or business process that involves the processing of personal data, a data protection impact assessment should be carried out (see also **Annex 2**) if the processing of personal data may pose a high risk to the data subject's personal rights. The high risk arises, for example, from the use of new technologies or the extensive processing of sensitive personal data.

The purpose of the data protection impact assessment is to identify and evaluate such high risks that new data processing may pose to the data subject's personal rights. When preparing the data protection impact assessment, measures can be identified and defined to avoid or reduce these risks. Further information and a questionnaire can be found in **Annex 2**.

6. Storage and erasure

As a rule, all stored personal data that is no longer required to fulfil the purpose of the processing must be permanently erased, unless a statutory retention period applies to the personal data in question or there is another legitimate reason for storing it. In order to fulfil this requirement, the Company has introduced (i) maximum retention periods for all stored personal data and (ii) regular review processes together with mechanisms for the cleansing of personal data.

The Company will retain data on its systems for the longer of the following periods: (i) for as long as is necessary or useful for the activity or services in question; (ii) any retention period required by law; or (iii) the end of the period in which litigation or investigations relating to services could arise (in Switzerland this is often 10 years). You must follow applicable record retention schedules and policies and destroy all media containing personal data in accordance with applicable record disposal policies, if any.

7. Disclosure of personal data abroad

In some cases, the Company may disclose personal data to recipients based in countries outside the European Union (EU), the European Economic Area (EEA) and Switzerland, whose laws often do not provide the same level of protection for personal data. In such cases, the Company must ensure that it takes appropriate security precautions that comply with the Company's legal obligations. In such cases, standard data protection clauses are often used that have been approved or recognised by the Federal Data Protection and Information Commissioner (FDPIC) (the European Commission's standard contractual clauses are important here). It is also conceivable that the data subject has expressly consented in writing to the disclosure of their data abroad (such consents must always be kept on file). Because criminal sanctions may also be imposed for the disclosure of data abroad, the Legal Department should be contacted before making problematic disclosures (e.g. if sensitive personal data is involved) in countries with inadequate data protection.

8. Training of employees and monitoring of order processors

All employees of the Company who process personal data are informed and trained about this Policy and the handling of personal data in compliance with data protection regulations.

In addition, DPAs must be concluded with all order processors (see above for the definition of order processor and its distinction from the controller). Attention should be paid to the clauses on data security (technical and organisational measures of the order processor), including the Company's audit rights and the rules on authorising the involvement of sub-order processors.

Employees who are responsible for supervising other employees or managing relationships with order processors are trained in how to supervise these employees and order processors.

9. Reporting a data security breach

Annex 1 contains the Directive on Reporting Data Security Breaches. This sets out definitions and binding action steps. The form contained in **Annex 1** must always be completed – even if it is not yet clear whether a data security breach has in fact occurred.

10. Monitoring compliance with and enforcement of regulations

The **General Counsel** is responsible for managing and overseeing the implementation of this Policy and for developing related operating procedures, processes, notices and guidelines.

If you believe that any provision of this Policy or any related policy, operating procedure, process or directive relating to the protection of personal data has been or is being violated, please contact the **Legal Department**.

The Company will conduct regular reviews and audits to verify compliance with this Policy. Employees who violate this Policy or a related policy, operating procedure or process for the protection of personal data may be subject to disciplinary action. Depending on the case, there could even be criminal consequences.

11. Annexes and other guidelines

In addition to this Policy, Annexes 1 to 3 and other Company policies relating to the processing of personal data must be observed and complied with at all times:

- Information Security Policy
- Directive on Reporting Data Security Breaches (incl. electronically fillable form) **(Annex 1)**
- Data Protection Impact Assessment Policy (incl. questionnaire) **(Annex 2)**
- Rules of conduct for requests for information incl. template for reply letter **(Annex 3)**

The Company reserves the right to issue new guidelines at any time. Employees will be informed of this in an appropriate manner.

12. Validity and document management

This directive is valid from 1 May 2024.

Earlier versions of this Policy will as a rule be retained for a period of 10 years.