HIAG

DATA PROTECTION POLICY

1. Purpose

HIAG Immobilien Holding AG ("Company") has adopted this Policy to govern the treatment of Company's customers' and employees' Personal Data. "Company" shall include all its subsidiaries. The loss of Personal Data can result in substantial harm to individuals, including embarrassment, inconvenience, and fraudulent use of the information. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that must be taken seriously at all times. Compliance with this Data Protection Policy ("Policy") is mandatory. Please note individuals' rights may vary depending on the applicable jurisdiction.

The purpose of the Policy is to:

- Define Personal Data and Sensitive Personal Data.
- Establish general principles for protecting Personal Data.
- Assign accountability for protection of Personal Data.

2. Scope

This Policy applies to all Company employees ("**You**"), agents, and representatives, including any contractor or third-party provider of services to the Company (**"Third-Party Service Provider"**) who have access to Personal Data the Company has collected or otherwise has in its possession. This Policy applies to all Personal Data collected, maintained, transmitted, stored, retained, or otherwise used by the Company regardless of the media on which that information is stored and whether relating to employees, customers, or any other person.

3. Definitions

"Controller" means the natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of Personal Data;

"Data Subject" means an identified or identifiable natural person about whom Personal Data is collected.

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

"Personal Data" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural. Such information includes, but is not limited to:

- Names;
- Addresses;
- Telephone numbers;
- Email addresses;
- Employee identification numbers;
- Government-issued identification numbers;
- User passwords or PINs;
- User identification and account access credentials, passwords, PINs and security question answers;
- Financial account numbers;
- Geolocation data; and
- Biometric, medical, health, or health insurance information.

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Sensitive Personal Data" means Personal Data that if lost, compromised, accessed, or improperly disclosed could result in harm, embarrassment, inconvenience, or unfairness to an individual and that therefore is subject to heightened protections. Examples of Sensitive Personal Data include, but are not limited to:

- An individual's government-issued identification number, including a social security number, driver's license number, or state-issued identification number;
- A financial account number, credit card number, or debit card number with or without any required security code, access code, personal identification number, or password, that would permit access to an individual's financial account;
- Biometric, medical, health, or health insurance information;
- Religious or philosophical beliefs or political opinions;
- Trade union membership;
- Sexual orientation; and
- Criminal records.

In most jurisdictions, the law will provide for the types of information that are subject to heightened protection. If you have any questions about whether any Personal Data qualifies as Sensitive Personal Data, you should contact the General Counsel.

"Security Incident" means any act or omission that compromises the security, confidentiality, or integrity of Personal Data or the physical, technical, administrative, or organizational safeguards the Company or a Third-Party Service Provider has put in place to protect Personal Data. The loss of or unauthorized access to, disclosure, or acquisition of Personal Data is a security incident.

4. Using, Handling, and Retaining Personal Data

4.1 Fair and lawful Processing

4.1.1 General

Whenever Company processes Personal Data, Company must ensure that the Processing happens in a lawful, fair, and transparent manner in relation to the Data Subject.

For certain Processing actions Company acts as Data Controller, joint Data Controller, or for others as Data Processor. Where Company acts in the capacity of Data Controller, Company must ensure it has the legitimate ground on which to collect and process Personal Data.

Where Company acts in the capacity of Data Processor, Company will generally process Personal Data on behalf of its customers. In those instances, customers will be responsible to ensure a legal basis for the Processing. However, contractual diligence is key, and Company's responsibilities should always be clearly defined in Company's agreements with customers.

4.1.2 Legal Basis

A legal basis is required to process Personal Data. Personal Data may be processed only if at least one of the following legal bases applies:

Consent: Consent is the most straightforward legal basis for the Processing of Personal Data. Important to note is that consent must be freely given, specific, informed and unambiguous. Consent can be given by written or oral statement or even by electronic means, such as ticking a box when visiting a website as long as it clearly indicates assent to the Processing. Silence, pre-ticked boxes or inactivity will not be seen as consent. Whenever Company process Sensitive Personal Data, explicit consent from the Data Subject is required. Consent can be withdrawn at any time and withdrawing the consent should be made as easy as granting consent.

Contractual necessity: Processing of Personal Data is justified if the Processing is required for the performance of a contract to which the Data Subject is a party to.

Compliance with legal obligations: Company is permitted to process Personal Data if the Processing is required to comply with a legal obligation.

Vital interests: Processing is permitted if it is necessary to protect the vital interests of the Data Subject or those of another person.

Public interest: Public interest covers Processing that is necessary for some public interest. Examples include taxation, crime reporting, public health and quality and safety of products.

Legitimate interest: A legitimate interest can be described as a benefit to a company, or to a society as whole, which can be derived from Processing Personal Data. Whenever Company wants to use legitimate interest as a basis for Processing, Company must ensure that a balance is struck between Company's interest and the rights and interests of the Data Subject.

4.2 Notice and Collection

It is Company policy that whenever it collects Personal Data for any purpose, including for human resources or employment purposes, it must inform the Data Subject of how it will use, process, disclose, protect, and retain that Personal Data by presenting a privacy policy or privacy notice to the individual at the time the individual provides the Personal Data. You may only collect Personal Data in compliance with applicable Company policies, notices, and Data Subject consent, and the Personal Data collected must be limited to that which is reasonably necessary to accomplish the Company's legitimate business purposes or as necessary to comply with law.

4.3 Access, Use and Sharing of Personal Data

You may only access Personal Data when the information relates to and is necessary to perform your job duties. You may not access Personal Data for any reason unrelated to your job duties. You may not use Personal Data in a way that is incompatible with the notice given to the Data Subject at the time the information was collected. If you are unsure about whether a specific use or disclosure is appropriate, you should consult with the General Counsel. You may only share Personal Data with another Company employee, agent, or representative if the recipient has a job-related need to know the information. Personal Data may only be shared with a Third-Party Service Provider if it has a need to know the information for the purpose of providing the contracted services and if sharing the Personal Data complies with the privacy notice provided to the Data Subject.

4.4 Accuracy

You must collect, maintain, and use Personal Data that is accurate, complete, and relevant to the purposes for which it was collected.

4.5 Security

You are responsible for protecting Personal Data. Company has implemented an Information Security Policy (ISP) that sets forth technical, administrative, and physical safeguards for the protection of Personal Data. You must follow the security procedures set out in the ISP at all times. You must exercise particular care in protecting Sensitive Personal Data from loss, unauthorized access, and unauthorized disclosure.

4.6 Accountability

Whenever Company acts as Data Controller, Company must be able to demonstrate compliance with the principles of Personal Data protection as defined in the GDPR and other applicable data protection laws. As an organization, Company will assess current practices and develop an adequate Personal Data privacy governance structure. Company has created a Personal Data inventory and use appropriate organizational and technical measures to ensure compliance with the Personal Data protection principles. All employees, agents, and representatives, including any contractor or third-party provider will abide by this principle by obtaining appropriate consents, complying with the incident reporting procedures (reporting can be done by consult with the General Counsel) and by submitting every new Processing of Personal Data, for assessment (Privacy Impact Assessment, see below) prior to engaging it.

4.7 Transparency

When Processing Personal Data, Company must be transparent. Transparency revolves around the Data Subject's right to maintain control over his / her Personal Data and requires Company to take the steps to ensure the necessary information is shared with the Data Subject. The Data Subject must be informed about:

- Who the Data Controller is;
- Source of the Data; purposes of the Processing; legal basis thereof and interests pursued by the Data Controller or third party, where relevant;
- Whether providing Personal Data is a requirement, why and what are the consequences of not providing;
- Recipients or their categories;
- Retention periods or, when not possible, criteria for their determination;
- Rights of the Data Subjects;

- Transfers of Personal Data to third countries or international organizations, including appropriate safeguards.

Ultimately, acting in a transparent manner means that Company should share with the Data Subject any information relating to the Processing and that Company makes that information easily accessible, easy to understand in clear and plain language. Company must make the Data Subject aware of the risks, rules, safeguards and rights relating to the Processing. Whenever Personal Data is collected through Company's website, this information is given in the form of a privacy notice (see section 4.2).

4.8 Data Subject's Rights

Individuals have rights when it comes to how their Personal Data is handled. These rights may vary depending on the applicable jurisdiction, but may include for example:

4.8.1 Primacy of Legal and Contractual Requirements

While the GDPR has allocated a set of robust rights to Data Subjects, it is important to note that those rights are not absolute and that legal or contractual requirements can have precedence over the rights of a Data Subject.

4.8.2 Right of Access and Rectification

All individuals have the right to establish whether Personal Data relating to them is being processed or not. They also have the right to obtain a copy of the Personal Data and additional information relating to the Processing (see section 4.8.6, Transparency). In particular, Company has an obligation to make them aware of the existence of additional rights, such as the rights to erasure and objection.

If a Data Subject discovers errors in the Personal Data that is being processed, it has the right to rectification of the Data without undue delay and free of charge. Likewise, the Data Subject has the right to complete the Personal Data if it is incomplete. It is Company's responsibility to take reasonable measures to facilitate these rights when acting as Data Controller. Should a Data Subject submit a request for access to his / her Personal Data, then this request should be met within one month upon receipt of the written request.

4.8.3 Right to be Forgotten (Right of Erasure)

A Data Subject has the right to have his / her Personal Data erased and no longer processed. This request can be made because (i) the Processing is no longer necessary in light of the purpose for which the Personal Data is collected or (ii) the Data Subject has exercised his / her right to withdraw his consent or (iii) the Personal Data is processed unlawfully or (iv) the erasure is mandated by law.

Whenever Company acts as Data Controller and has made Personal Data public, then Company must notify any one to whom Company has disclosed the Personal Data of this request of erasure, unless this would be impossible or involve a disproportionate effort or unless Company is either establishing, exercising or defending a legal claim.

4.8.4 Right to Object

The right to object is closely linked and similar to the right to be forgotten. Any Data Subject has the right to object to direct marketing at any time (unsubscribe) and in that event, Company is obliged to stop using the Personal Data for marketing purposes. The right to object can also be exercised in the instances as defined the right to be forgotten.

4.8.5 Right to Data Portability

Company has to comply with a Data Subject's request to provide him / her with a copy of his / her Personal Data. When doing so, Company must ensure that this happens in a structured, commonly used manner. Company also has to ensure that the Data can be consulted in a machine-readable format. The purpose of this right is to allow the Data Subject to transfer his / her Personal Data to a different controller.

4.8.6 Transparency

It should again be stressed that the increased transparency required under the GDPR means that individuals are required to be clearly informed of the existence of their rights.

4.8.7 Marketing

When Data Subjects register on Company's website or sign up for marketing material, they are giving consent to receive (e)mails from Company informing them of Company's services, future events and other activities Company believes will be of interest to them.

As a rule, Company should ensure that all of its marketing activities (i) are based on consent, (ii) clearly state for which purpose a Data Subject's details will be used, (iii) provide a simple way for Data Subjects to opt out / unsubscribe of marketing messages and (iv) have a process in place for dealing with complaints.

4.8.8 Further Information regarding Rights of Data Subjects

You must comply with applicable laws regarding the rights of Data Subjects. If you are unsure of the applicable legal requirements, or if you receive a request or complaint from a Data Subject regarding the handling of his or her Personal Data, please contact the General Counsel.

5. Privacy Impact Assessment

Prior to launching any proposed new system and business process involving Personal Data, a privacy impact assessment should be performed (see Privacy Impact Assessment Policy). The purpose of the privacy impact assessment is to evaluate the way a system or process collects, uses, stores, transfers and deletes Personal Data.

The objective of the privacy impact assessment is to identify potential confidentiality or privacy risks in the system or process and to examine and evaluate alternative ways for Processing Personal Data to mitigate those risks.

6. Retention and Disposal

As a rule, all Personal Data collected which is no longer required to achieve the purpose of the Processing should be permanently deleted unless the Personal Data is bound by a legal retention period or any other ground for retention. To comply with this requirement, Company should implement (i) maximum retention periods for all Personal Data collected, and (ii) regular review processes together with mechanisms of Personal Data cleansing.

Company will hold Data on its systems for the longest of the following periods: (i) as long as is necessary or useful for the relevant activity or services; (ii) any retention period that is required by law; or (iii) the end of the period in which litigations or investigations might arise in respect of any services. You must follow the applicable records retention schedules and policies and destroy any media containing Personal Data in accordance with the applicable records disposal policy, if available.

7. International Transfers

In some cases, Company might transfer Personal Data to recipients that may be based in countries outside of the European Union and Switzerland whose laws may not provide the same level of Personal Data protection. In such cases, Company will ensure that there are adequate safeguards in place that comply with Company's legal obligations to protect Personal Data. The adequate safeguard might be a Personal Data transfer agreement with the recipient based on standard contractual clauses approved by the European Commission for transfers of Personal Data to third countries or reliance on Privacy Shield.

8. Training Employees and Supervising Contractors

All Company employees who have access to Personal Data must be educated and trained on this Policy and the treatment of Personal Data. In addition, whenever Personal Data is entrusted to a Third-Party Service Provider, proper management and supervision over the outside party's handling of that Personal Data must be ensured through appropriate contracts. Employees with responsibility for supervising other employees or managing Third-Party Service Provider relationships must be trained on supervision over those employees and Third-Party Service Providers.

9. Reporting a Security Incident

If you know or suspect that a Security Incident has occurred, do not attempt to investigate the matter yourself. Immediately contact the General Counsel. You should preserve all evidence relating to the potential Security Incident.

10. Monitoring Compliance and Enforcement

The General Counsel is responsible for administering and overseeing implementation of this Policy and, as applicable, developing related operating procedures, processes, policies, notices, and guidelines. If you are concerned that any provision of this Policy, or any related policy, operating procedure, process, or guideline designed to protect Personal Data, has been or is being violated, please contact the General Counsel. Company will conduct periodic reviews and audits to assess compliance with this Policy. Employees who violate this Policy and any related guidelines, operating procedures, or processes designed to protect Personal Data and implement this Policy may be subject to discipline.

11. Related Policies

Other Company policies also apply to the collection, use, storage, protection, and handling of Personal Data and may be relevant to implementing this Policy. You should familiarize yourself with these policies, including:

- Information Security Policy (Annex 1).
- Data Breach Notification Policy (Annex 2).
- Privacy Impact Assessment Policy (Annex 3).
- Data Subject Access Request Procedure (Annex 4).

12. Amendment and Revision

This Policy may be revised from time to time.

HIAG

Information Security Policy (ISP)

1. Purpose, scope and users

The aim of this top-level Policy is to define the purpose, direction, principles and basic rules for information security management.

Users of this document are all employees of HIAG, as well as relevant external parties.

2. Basic information security terminology

Confidentiality – characteristic of the information by which it is available only to authorized persons or systems.

Integrity – characteristic of the information by which it is changed only by authorized persons or systems in an allowed way.

Availability – characteristic of the information by which it can be accessed by authorized persons when it is needed.

Information security – preservation of confidentiality, integrity and availability of information.

3. Managing the information security

3.1 Objectives and measurement

General objectives for the information security management are the following: creating a better market image and reducing the damage caused by potential incidents; goals are in line with the organization's business objectives, strategy and business plans.

All the objectives must be reviewed at least once a year.

HIAG will measure the fulfilment of all the objectives. Executive Management is responsible for setting the method for measuring the achievement of the objectives – the measurement will be performed at least once a year and Executive Management will analyse and evaluate the measurement results and report them to the Board of Directors as input materials for the Management review.

3.2 Information security requirements

This Policy must be compliant with legal and regulatory requirements as well as with contractual obligations relevant to the organization and its customers in the field of information security and protection of Personally Identifiable Information (PII).

3.3 Information security controls

The process of selecting the controls (safeguards) is defined in the Internal Control System (IKS).

The selected controls and their implementation status are listed in the IKS.

3.4 Responsibilities

Responsibilities for the Information Security are the following:

- Executive Management is responsible for ensuring that all necessary resources are available
- Executive Management is responsible for operational coordination as well as for reporting about the performance of the information security according to this Policy.
- Executive Management is responsible for operational security of all provided services and internal systems as well as for reporting about the services' and internal systems' security performance.
- Executive Management must review the IS reports at least once a year or each time a significant change occurs, and prepare minutes from that meeting.
- Executive Management will implement information security training and awareness programs for employees
- the protection of integrity, availability, and confidentiality of assets is the responsibility of the owner of each asset
- all security incidents or weaknesses like for instance suspicion of a data breach must be reported to Executive Management and must be registered
- Executive Management will define which information related to information security will be communicated to which interested party (both internal and external), by whom and when
- Executive Management is responsible for ensuring the proper designation of responsibilities to customers, partners, suppliers, and other third parties who have a role in information security management
- Executive Management is responsible for adopting and implementing the Training and Awareness Plan, which applies to all persons who have a role in information security management

3.5 Policy communication

Executive Management has to ensure that all employees of HIAG, as well as appropriate external parties are familiar with this Policy.

4. Support for IS implementation

Hereby the Board of Directors declares that information security and continual improvement will be supported with adequate resources in order to achieve all objectives set in this Policy, as well as satisfy all identified requirements.

5. Validity and document management

This document is valid as of 25.5.2018.

The owner of this document is the General Counsel, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- number of employees and external parties who have a role in the IS, but are not familiar with this document
- non-compliance of the IS with the laws and regulations, contractual obligations, and other internal documents of the organization
- ineffectiveness of IS implementation and maintenance
- unclear responsibilities for IS implementation

Previous versions of this policy must be stored for a period of 5 years, unless specified otherwise by legal or contractual requirement.

HIAG

Data Breach Notification Policy

1. Purpose

Company is taking every care to protect Personal Data from Security Incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and financial costs.

This Data Breach Notification Policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and Security Incidents across Company.

This Data Breach Notification Policy relates to all Personal Data and Sensitive Personal Data held by Company regardless of format.

The objective of this Data Breach Notification Policy is to contain any breaches, to minimize the risk associated with the breach and consider what action is necessary to secure Personal Data and prevent further breaches.

For the purpose of this Data Breach Notification Policy, Security Incidents include both confirmed and suspected incidents.

2. Types of Breach

A Security Incident in the context of this Data Breach Notification Policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to Company's information assets and reputation.

A Security Incident includes but is not restricted to, the following:

- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record);
- equipment theft or failure;
- system failure;
- unauthorized use of, access to or modification of data or information systems;
- attempts (failed or successful) to gain unauthorized access to information or IT system(s);

- unauthorized disclosure of sensitive / confidential data;
- website defacement;
- hacking attack;
- unforeseen circumstances such as a fire or flood;
- human error;
- "blagging" offences where information is obtained by deceiving the organization who holds it.

3. Reporting an incident

Everyone who accesses, uses or manages Company's information is responsible for reporting data breach and Security Incidents immediately to the Data Protection Officer ("**DPO"**). If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process (attached to this Data Breach Notification Policy).

You should be aware that any breach of Data Protection Regulations may result in Company's disciplinary procedures being instigated.

4. Containment and recovery

The DPO will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the DPO in liaison with relevant officer(s) to establish the severity of the breach and who will take the lead investigating the breach as the lead investigation officer ("**LIO**") (this will depend on the nature of the breach; in some cases, it could be the DPO).

The LIO will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

Advice from experts across Company may be sought in resolving the incident promptly.

The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

5. Investigation and risk assessment

An investigation will be undertaken by the LIO immediately and wherever possible, within 24 hours of the breach being discovered / reported.

The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:

- the type of data involved;
- its sensitivity;
- the protections that are in place (e.g. encryptions);
- what has happened to the data (e.g. has it been lost or stolen;
- whether the data could be put to any illegal or inappropriate use;
- Data Subject(s) affected by the breach, number of individuals involved and the potential effects on those Data Subject(s);
- whether there are wider consequences to the breach.

6. Notification

The LIO or the DPO, in consultation with relevant colleagues will establish whether the Information data protection authority will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection Regulations;
- whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);
- whether notification would help prevent the unauthorized or unlawful use of Personal Data;
- whether there are any legal / contractual notification requirements;
- the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

Individuals whose Personal Data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact Company for further information or to ask questions on what has occurred.

The LIO or the DPO must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

The LIO or the DPO will consider whether the communications team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

A record will be kept of any Personal Data breach, regardless of whether notification was required.

7. Evaluation and response

Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- where and how Personal Data is held and where and how it is stored;
- where the biggest risks lie including identifying potential weak points within existing security measures;
- whether methods of transmission are secure; sharing minimum amount of data necessary;
- staff awareness;
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the General Counsel.

8. Amendment and Revision

This Data Breach Notification Policy may be revised from time to time.

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify the Data Protection Officer and complete Section 1 of this form and email it to the Data Protection Officer.

Section 1: Notification of Data Security Breach	To be completed by person reporting incident
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any Personal Data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	
Contact details of person reporting incident (email address, telephone number):	

Section 2: Assessment of Severity	To be completed by the Lead Investigation Officer in consultation with the person of the area affected by the breach and if appropriate IT where applicable.

Details of the IT systems, equipment, devices, records involved in the security breach:

Details of information loss:

What is the nature of the information lost?

How much data has been lost? If laptop lost / stolen: how recently was the laptop backed up onto central IT systems?

Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for Company or third parties?

How many Data Subjects are affected?

Is the data bound by any contractual security arrangements?

What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:

HIGH RISK personal data

- Sensitive Personal Data (as defined in the Data Protection Regulations) relating to a living, identifiable individual's
    a) racial or ethnic origin;
    b) political opinions or religious beliefs;
    c) trade union membership;
    d) genetics;
    e) biometrics (where used for ID purposes)
    f) health;
    g) sex life or sexual orientation
- Information that could be used to commit identity fraud such as; personal bank account and other financial information;

national identifiers, such as copies of passports and visas; – Personal information relating to vulnerable adults and children; – Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed; – Security information that would compromise the safety of individuals if disclosed. Data Protection Officer or Lead Investigation Officer to consider whether it should be escalated to General Counsel.	
Section 3: Action taken	To be completed by Data Protection Officer or Lead Investigation Officer
Incident number	e.g. year/001
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	Yes / No
If YES, notified on (date):	
Follow up action required / recommended:	
Reported to Data Protection Officer and Lead Officer on (date):	

HIAG

Policy for Completing a Privacy Impact Assessment ("PIA") of Systems and Processes

New systems and processes may require data to be processed, stored and accessed anywhere within Company or managed on behalf of Company by external service providers. The following PIA has been created to understand and document the various data flows that may be created as a result of a new system or process and ensure all appropriate data privacy compliance obligations have been taken into account.

For each of these systems / processes, Company will work with the system / process owners to:

- Clarify what the system / process involves
- Establish what impact (if any) there is upon the system / process and conduct a PIA of current practices against Company's privacy requirements
- Develop appropriate data privacy action items for the system / process and ensure they are implemented. The action items may include such things as:
    - Data Privacy Notices for system users;
    - Suggested data retention standards for Personal Data processed in the system if none exist;
    - Detailed background analysis and guidance containing the information required by Company;
    - High level guidelines for system users.

Privacy Impact Assessment (PIA) Questionnaire

System / Process: (Please expand any acronyms used in the name system.)

Template completed by:

(Please provide the name of the person completing this Questionnaire and also the name of the system owner if different to the person completing this Questionnaire.)

Step One - Assess the current system / process.

NB – Please ensure you refer to the agreed key definitions when completing the PIA Questionnaire especially in relation to the definition of 'personal data'.

	Question	Discussion / issues
	Fair and Lawful processing requirements	
1.	Is Personal Data and confidential data Processed (see definition of "Personal Data" and "Processed" in the HIAG Data Protection Policy)	*Answer "Yes" or "No" here only.*
2.	Is Sensitive Personal Data Processed? If yes, please list the data classes.	*Answer "Yes" or "No" here.* *If you answer "Yes", please provide details of the specific Sensitive Personal Data elements which are processed in the system. "Sensitive Personal Data" means Personal Data of an individual consisting of information as to* • *the racial or ethnic origin of the data subject,* • *his / her political and philosophical opinions,* • *his / her religious beliefs and activities or other beliefs and activities of a similar nature,* • *whether he or she is a member of a trade union and his / her position to trade unions,* • *his / her physical or mental health or condition,* • *his / her sexual life and private sphere,* • *his / her administrative or criminal proceedings and convictions,*

		• *his / her social security files.* *Also, when answering this Question, please indicate whether the system has "free text" areas where it could be possible for an individual to enter Sensitive Personal Data if they choose to do so.*
3.	What sort of Personal Data and confidential data is it (names, addresses, contact details, gender, medical history, salary / performance data, etc.)? Please provide a list of the data classes / categories for the process / system. Where possible please provide a data dictionary.	*Personal Data could include such things as:* • *Name (first, last name)* • *Email address* • *Contact details* • *Gender* • *Date of Birth* • *Salary* • *Performance data* • *Education* • *Passport or ID details* • *System log-in details (username and password)* *If confidential customer engagement information is also processed in the system, please provide details.* *Please provide an Excel or Word doc schedule setting out all of the data elements which are processed in the system.*
4.	Where is the Personal Data – including Sensitive Personal Data and confidential data – sourced from? (Provide details of other processes / systems / data feed etc.)	*The data could be manually entered into the system directly by Company, employees or contractors.* *The data could also be entered into the system via a feed from any one or more of the following "upstream" systems:* *The data could also be manually entered into the system directly by Company's customers or other third parties.*

5.	Describe the purpose of the Processing and outline of the process, include the key elements.	*Summarize the purpose of the system in one sentence and then expand your answer to provide further general details of the business need for the system, the purpose of the processing and an outline of the process (and a flow chart if available).* *You may have details of the business need for the system and / or the purpose of the system within the introductory sections of PowerPoint presentations, system specifications documents, vendor RFP's or user manuals for the system. You should indicate who is implementing the system and the expected benefit to Company (e.g. increased revenues or efficiencies) which is hoped to be achieved from its deployment.*
6.	Clarify who the data covers (employees, contractors, customers, suppliers, ex-employee's etc. These are just examples and not an exhaustive list).	*The Personal Data which is processed in the system could relate to one or many of the following:* • *Company employees* • *Company's contractors* • *Former Company's contractors* • *Customers* • *Former customers* • *Vendors* • *Former vendors* • *Others (provide details)*
7.	Are Data Subjects aware of the Processing of his / her Personal Data?	*The answer to this Question will likely be one of the following responses:* • *No* • *Yes, a privacy notice will be drafted and will be made available in the system* • *Yes, a privacy notice is available (note: please provide us a copy to review)* • *Yes, the obligation is on the customers or vendor to notify individuals* • *Yes, as part of their employment contract or staff manual* • *Yes, other (details)*

8.	What is the purpose communicated to the Data Subjects (see definition below) upon collection of the Personal Data?	*The answer to this Question will depend on the response given in Question 7 above.* *Eg. From the privacy notice, users of the system will understand that the purpose of the system is [repeat the one sentence purpose of the system as set out in Question 5 above].*
	Data Management – ie. Accuracy, retention policy etc.	
9.	Who (which legal entity) has responsibility for the data management?	*The answer to this Question will likely be one of the following (please choose appropriate response):* • *An external vendor licenses the system to us, and we are responsible for data management.*
10.	What are the procedures for managing the data held on the system? i.e. Who is responsible for granting access to the data and keeping it up to date?	*Provide details on the process for granting users access to the system (eg. which specific named team is responsible for granting user access to the system – how many people are in this team and where are they located?)* *Data may be kept up to date in the system by one or more of the following methods:* • *By data feeds from upstream systems* • *Manually updated by an engagement team member* • *Manually updated by system administrators* • *Manually updated by users of the system (customers, Company or third party)* • *The data processed is a "snapshot in time" and is not updated once uploaded / at the conclusion of an engagement* *What is the process for withdrawing access rights when access is no longer needed (for example, if an employee leaves us or moves to another role for which access is no longer required)?*

11.	Does the process feed into any additional process / system?	*Answer "Yes" or "No".* *If "Yes", provide the names of the downstream systems from which this system feeds and indicate whether this is a manual feed or an automatic feed. Include details of any reporting tools which display data which is processed in the system.*
12.	How is the Personal Data used? (Explain how accuracy of the Personal Data is maintained.)	*You have provided details of the purpose of the system in Question 5 above. Now explain how the Personal Data which is processed in the system enables us to achieve this purpose. For example, the Personal Data may be used in the system to identify individuals to whom we are providing professional services using the system.*
13.	Are there any interdependencies with other systems / processes? ie. where changes to one database automatically feed through and are reflected in another.	*Provide details of any automatic feed (upstream or downstream) from the system into any additional process / system.*
14.	Is there a data retention policy linked to the process / system? If so provide details eg, retention period, access rights, disposal of data etc.	*Provide details of the procedures or policies for data retention and data disposal in the system including:* • *Applicable retention period / policy for retention* • *Process for deleting data (manual or automated process?)* • *Will data be retained in a separate archive system before it's permanently deleted?* *If there is currently no data retention policy for the system then one will need to be established in order to comply with data privacy laws.*
	System Ownership – Hardware and Software	

15.	Which legal entity owns the system associated with the process?	*The answer to this Question will likely be one of the following (please choose appropriate response):* • *The system has been developed internally by us and is therefore owned by us.*
16.	Does the same legal entity own the hardware / servers etc? (Please provide details.)	*The answer to this Question will likely be one of the following (please choose appropriate response):* 1. *The system is hosted within our infrastructure:* • *Data Center [country]* • *Data Center [country]* • *Data Center [country]* 2. *The system is hosted externally by the vendor or its third-party hosting provider [provide details of location (country, city)].*
17.	Where are the servers housed, e.g. US.	*Following from your response to Question 16 above, the answer to this Question will likely be either:* 1. *The Data Centre in [[location – country and city]; or* 2. *The vendor's data centre in [location – country and city]*
	Transfers outside of Company	
18.	Is the Personal Data transferred outside of Company?	*Answer "Yes" or "No".* *Note that where we host the system, any access by external parties to Personal Data which is Processed or stored within the system will constitute a transfer of the Personal Data outside of Company and therefore needs to be listed here.*
19.	Who is the Personal Data transferred to? Include all external third parties, eg. Government bodies, regulators, data processors etc.	*If you answered "Yes" in Question 18 above, clarify the individuals outside Company who have access to the data in the system. This could include the following:* • *Customers* • *Regulator* • *Vendor for providing hosting or IT support*

		• *Other [provide details]*
20.	What Personal Data is transferred?	*If you answered "Yes" in Question 18 above, the answer to this Question could be:* • *All of the data elements which are listed in Question 2 and 3 above; or* • *A subset of the data elements listed in Question 2 and 3 above [provide details].*
21.	What is the purpose of the transfer?	*If you answered "Yes" in Question 18 above, the purpose of transfer could be:* • *Provision of services to customers* • *Provision of other administrative and IT support services* • *Other [provide details]*
22.	Is there a contract with the third party? (Please provide a copy for assessment.)	*Please provide copy of the contract with the vendor where available so we can check to see if it contains appropriate confidentiality and data privacy provisions, including EU Model Clauses or a Data Transfer Agreement.*
	Security requirements – access to data	
23.	What technical and organization security measures does the system have to protect the Personal Data, confidential data and Sensitive Personal Data against accidental loss, destruction, damage or unlawful processing?	*Please choose one of the following options:* • *The system has been reviewed by [name] IT Security and the system is compliant with our IT security policies.* • *The system is in the process of being reviewed and will only be deployed once IT Security has confirmed compliance with our IT security policies.*
24.	Who has access to the Personal Data?	*Provide details showing which persons, positions or employee categories ("Roles") will have access to which elements or records of data in the system. Please clarify*

		if individuals outside of Company might have access to the data in the system.
25.	What categories of access do individuals have e.g., read only, edit, delete etc.?	*Explain for each of the recipient Roles listed in Question 24 above:* • *Where they are located (country);* • *What the purpose is for which they need access; and* • *What level of access rights they will have (read-only, edit, delete etc).* *Also, please provide us with a schedule showing each Role and its corresponding access rights which should be available by the system vendor or our IT developer.*
26.	Is it possible to extract a personality profile should there be a request to do so?	*The answer to this Question will likely be one of the following (please choose appropriate response):* • *No.* • *Yes – an individual's name can be readily searched / looked up in the system in case that individual makes a subject access request for details of his or her information which is in the system.*
	Overseas Transfers	
27.	Is the Personal Data transferred outside the EEA?	*Answer "Yes" or "No".* *Note when answering this Question that any access to Personal Data which is stored within the EEA by parties who are located outside of the EEA will constitute a transfer of Personal Data outside of the EEA.*
28.	Where is the Personal Data transferred to?	*If you answered "Yes" in Question 27 above, the transfer could be to the location of the individuals who access the system from outside of the EEA.*
29.	What is the purpose of the transfer, eg storage, additional access requirements etc.?	*If you answered "Yes" in Question 27 above, the purpose of transfer outside of the EEA could be one or more of the following:*

		• *To enable individuals to use the system in accordance with the purpose set out in Question 5 above.* • *The provision of services to customers* • *Provision of other administrative and IT support services* • *Other [provide details]*
30.	What security measures are in place to ensure safe transfer of both Personal Data and Sensitive Personal Data?	*Please choose one of the following options:* • *The system has been reviewed by our IT security and the system is compliant with our IT security policies.* • *The system is in the process of being reviewed and will only be deployed once our IT security has confirmed compliance with our IT security policies.*
31.	What controls are in place to prevent further onward transfers of the Personal Data?	*Please choose one or both of the following responses:* • *The terms of the service agreement between us and the system vendor will determine any further onwards transfers of Personal Data or confidential information. Access to this information is restricted to those employees of the vendor with a defined business need.* • *The system owners understand the significance of maintaining data privacy and confidentiality and would query any requests or attempts to transfer data to another system or otherwise download information from the system unless it had first been approved from an IT and privacy standpoint.*

HIAG

Data Subject Rights Request Procedure

Data Protection law gives individuals rights when it comes to how their Personal Data is handled. These rights may vary depending on the applicable jurisdiction (see HIAG Data Privacy Policy section 4.8).

This Data Subject Rights Request Procedure explains how Company deals with a subject rights request relating to such personal data (referred to as "**valid request**" in this Procedure).

An individual making a valid request to Company is entitled to benefit of the rights given by applicable data protection regulations.

1. Request

The request must be made in writing, which can include email. Under normal circumstances no fee will be applied but this will be left to the discretion of Company and in accordance with local applicable law.

Company must respond to a valid request within 30 calendar days (or any shorter period as may be stipulated under local law) of receipt of that request. Company is not obliged to comply with a subject request unless Company is supplied with such information which it may reasonably require in order to confirm the identity of the individual making the request.

2. Procedure

2.1 Receipt of a Subject Rights Request

If any employee or subcontractor of Company receives any request from an individual for their personal data, they must pass the communication to the General Counsel upon receipt indicating the date on which it was received together with any other information which may assist Company to deal with the request.

2.2 Initial Steps

Company will make an initial assessment of the request to decide whether it is a valid request and whether confirmation of identity, or any further information, is required.

Company will then contact the individual in writing to confirm receipt of the subject rights request, seek confirmation of identity or further information, if required, or decline the request if permitted by applicable law.

2.3 Exemptions to Subject Rights Requests

A valid request may be refused on the following grounds:

(i) if the refusal to provide the information is consistent with applicable data protection law within that jurisdiction, or;

(ii) where the subject access request does not fall within the above and:

- if, in the opinion of Company, it is necessary to do so to safeguard the legitimate business interests of Company, national or public security, defence, the prevention,

investigation, detection and prosecution of criminal offences, for the protection of the data subject or of the rights and freedoms of others; or

- where the Personal Data does not originate from a country that provides data subjects with a certain requested right and granting of such right requires Company to use disproportionate effort.

2.4 The Search and the Response

Company will arrange a search of all relevant electronic and paper filing systems.

The information requested will be collated by Company into a readily understandable format (internal codes or identification numbers used at Company that correspond to Personal Data shall be translated before being disclosed). A covering letter will be prepared by Company which includes information required to be provided in response to a subject rights request.

Where the provision of the information in permanent form is not possible or would involve disproportionate effort (if permitted by applicable law) there is no obligation to provide a copy of the information. The other information referred to above must still be provided. In such circumstances the individual may be offered the opportunity to have access to the information by inspection or to receive the information in another form.

2.5 Requests for Erasure, Amendment or Cessation of Processing of Information

If a request is received for the deletion of that individual's Personal Data, such a request must be considered and dealt with as appropriate by Company. If a request is received advising of a change in that individual's Personal Data, such information must be rectified or updated accordingly if Company is satisfied that there is a legitimate basis for doing so.

Where the processing undertaken by Company is required by law, the request will not be regarded as valid.

All queries relating to this procedure are to be addressed to the General Counsel.