Data Security Policy

We, the ***InnoFly Company Family***, recognize the importance of protecting personal data and are committed to respecting and safeguarding the privacy of our employees, customers, and business partners. In this policy, we outline the key aspects of the General Data Protection Regulation (GDPR), explain how we comply with its requirements, and detail how we maintain data protection within our InnoFly Company Family.

1 Why is the Data Security Policy important?

As part of our InnoFly Company Family, each of us is ***responsible*** for respecting and protecting the privacy of our customers, partners, and employees. Compliance with the GDPR is not only a legal obligation but also a central element of our ethical commitment and professional conduct.

The GDPR provides clear guidelines on how personal data should be handled while granting comprehensive rights to the individuals concerned. Violations of these regulations can lead to substantial fines and can severely damage the trust in our company. Moreover, legal actions could follow, negatively impacting our corporate image and market position.

Therefore, all employees are urged to take data protection seriously and actively contribute to the implementation of data protection measures. These measures include:

- Regularly ***reading and understanding our Data Security Policy***.
- ***Immediately reporting*** any suspicious activities or security breaches that could jeopardize personal data.
- ***Continuously training and raising awareness*** about the latest data protection regulations and practices.
- ***Strictly adhering to data handling and request*** procedures to ensure confidentiality and security.

2 General Information on the GDPR

The ***General Data Protection Regulation*** is a framework designed to protect the data of citizens in the European Union. This regulation applies whenever personal data of a person located in the EU is processed, regardless of whether the company processing the data is based inside or outside the EU. As soon as it involves data of individuals residing in the EU, the GDPR is applicable. For instance, even Amazon, an American company offering goods in Europe, is subject to the GDPR.

Personal data refers to any information relating to an identified or identifiable natural person. This can include data such as name, address, phone number, email address, date of birth, IP address, or biometric characteristics. According to the GDPR, this data must be specially protected as it can be traced back to a specific individual.

Data processing under the GDPR comprises any type of operation performed on an individual's personal data. This includes actions such as collecting, storing, organizing, using, transmitting, or deleting this data.

Let's imagine you check a box indicating that you accept the receipt of a company's newsletter. By doing so, you agree that your email address may be used and stored for this purpose. This company performs various activities with your email address:

- ***Collecting***: They capture your email address.
- ***Storing***: They store it in their database.
- ***Using***: They use the address to send you newsletters.

- ***Deleting***: If you decide you no longer want to receive newsletters and inform the company, they delete your email address from their database.

All these activities fall under the term "data processing." The GDPR ensures that at each of these steps, your data is handled securely, and you have control over what happens to it.

Current Practical Example	
Incident	Advertising without valid consent
Penalty	€ 1,2 million

3 Why is the GDPR compliance so important?

The protection of personal data is not only a ***legal obligation*** but also a ***sign of respect*** for individuals' privacy. Compliance with the GDPR demonstrates that a company handles data responsibly, which strengthens the trust of customers, employees, and partners. However, non-compliance can lead to significant consequences, including:

- ***Fines***: Companies can face penalties of up to €20 million or 4% of their global annual revenue, whichever amount is higher.
- ***Loss of Reputation***: Data breaches can severely damage a company's image, leading to customer loss and negative press.
- ***Legal Consequences***: Affected individuals can take legal action if they believe their data has been unlawfully processed.

Generally, the employer is liable for their employees' mistakes towards third parties. However, within an employment relationship, there are specific legal liability rules. Through the so-called internal damage compensation, the ***responsibility is shared between the employee and employer in case of employee*** misconduct, allowing the employer to reclaim the paid fine from the employee.

Violations of data protection regulations can have ***serious employment consequences***, such as warnings or even termination. For example, the Regional Labor Court of Cologne ruled that reading and printing an email clearly addressed to a colleague, as well as copying and passing on a colleague's private chat logs to third parties, can justify immediate dismissal without notice.

Another ruling by the Regional Labor Court of Berlin-Brandenburg in 2016 confirmed that the mass retrieval of registration data out of curiosity by an employee can justify immediate dismissal without notice, even if only a few people are affected.

Current Practical Example	
Incident	Imposed sanction for non-transparent data security policy
Penalty	up to €7 million

4 What rights do individuals whose data we store have?

The GDPR grants individuals in the EU various rights to give them control over their personal data. Here are these rights explained simply:

- ***Right of Access***: Individuals can request confirmation as to whether personal data concerning them is being processed. If so, they can request a copy of this data and receive information on how and for what purposes the data is being processed.
- ***Right to Rectification***: If the stored data is incomplete or incorrect, individuals have the right to request its correction or completion.
- ***Right to Erasure*** (Right to be Forgotten): Under certain conditions, individuals can request the deletion of their data. This is particularly applicable when the data is no

longer necessary for the original processing purposes or when consent for processing has been withdrawn.

- ***Right to Restrict Processing***: Under certain circumstances, individuals can request that the processing of their data be restricted. This means that the data can be stored but not further processed.
- ***Right to Data Portability***: Individuals have the right to receive their data in a structured, commonly used, and machine-readable format. They also have the right to have this data transmitted to another controller without being hindered by the organization providing the data.
- ***Right to Object***: Individuals can object to the processing of their data, particularly if it is for marketing purposes or due to a specific situation.
- ***Right to File a Complaint***: Individuals have the right to lodge a complaint with the supervisory authority (in Austria: Data Protection Authority, Barichgasse 40-42, 1030 Vienna, Email: dsb@dsb.gv.at) if they believe that the processing of their personal data violates the GDPR.

Current Practical Example	
Incident	Incorrect negative disclosure and non-compliance with response deadline
Penalty	€ 46,500

5 Technical & Organizational Security Measures

Due to the GDPR, companies are required to implement technical and organizational security measures to protect the personal data of their customers, employees, and business partners. These measures aim to safeguard data from unauthorized access, loss, or misuse.

Here are the key obligations that arise from this:

- ***Access Control***: Ensure that only authorized personnel have access to the data. This can be achieved through password protection, biometric recognition, or security cards.
- ***Data Backup***: Regular data backups are essential. These backups should be stored in secure locations and encrypted to enable data recovery in the event of data loss.
- ***Encryption***: Sensitive data should be encrypted both during transmission and storage to protect it from unauthorized access.
- ***Monitoring and Logging***: Companies must monitor and log access to personal data to trace possible security incidents.
- ***Training and Awareness***: Employees must be regularly informed and trained on data protection policies and the secure handling of personal data.
- ***Privacy Impact Assessment (PIA):*** For certain data processing activities that pose a high risk to the rights and freedoms of individuals, companies must conduct and document a PIA.
- ***Emergency Management***: A plan should be in place that defines actions in the event of data breaches and security incidents. This includes notifying the affected individuals and the competent data protection authority within 72 hours.

Every employee is ***responsible for protecting data***. A single mistake or act of negligence can have serious consequences. By ensuring that all employees are aware and trained, the risk of such errors is minimized. In the event of a security incident, it is crucial that all employees know how to respond and what steps to take. A well-informed and coordinated team can act quickly and efficiently to mitigate damage and ensure compliance with legal reporting obligations.

The successful implementation of these measures critically depends on the collaboration of all employees. ***Data protection*** is not just the responsibility of the IT department or the data protection coordinator; it ***concerns every single employee*** in the company.

Current Practical Example	
Incident	Imposed sanction for insufficient technical and organizational security measures
Penalty	up to €5 million

6 Data-Breach-Notification Duty

If it becomes known that personal data has been compromised due to a security deficiency in the implemented technical and organizational measures (=***data breach***), the affected individuals must be informed immediately.

- Data misuse can occur due to the following events:
- Unauthorized access to data, e.g., by external attackers (hacking attack) or unauthorized employees
- Theft of IT components and data carriers (PCs, notebooks, USB sticks, paper documents, printouts, etc.)
- Loss of IT components and data carriers (notebooks, USB sticks, smartphones, etc.)
- Incorrect addressing, sending emails to a large distribution list with "cc" instead of "bcc"

Moreover, for a data breach to be reportable, there must be an objective breach of personal data protection. Mere suspicion is not sufficient. It is not decisive whether a third party has actually gained knowledge of the data.

It should be noted that the damage does not need to have already occurred. It is sufficient that there is the possibility that damage (financial, reputational, or physical harm to the affected individuals) could arise in the future. However, this potential damage must be significant; minor damage does not create an obligation to inform.

In the event of a data breach, both the data protection authority and the affected individuals must be notified ***within 72 hours***. The reporting period begins ***from the moment anyone*** in the company ***becomes aware*** of the significant facts of the data breach. This deadline also applies on weekends and even during holidays like Easter and Christmas. Therefore, upon learning of such facts, the data ***protection coordinator must be informed immediately***.

The notification of the affected individuals can be made in any possible form. In addition to direct communication methods, such as by letter or email, publication in daily newspapers is also conceivable.

Current Practical Example	
Incident	Imposed sanction for delay in the 72-hour reporting obligation
Penalty	up to €500,000

7 Handling Data Protection Requests

Responding to inquiries or complaints regarding data protection is the responsibility of the Data Protection Coordinator. Incoming inquiries should be promptly forwarded to datenschutz@innofly.at.

When dealing with requests for information addressed to you, please strictly adhere to the following guidelines:

- ***Principle of Data Confidentiality***: Providing information is generally prohibited unless there is a legal basis for the data disclosure.
- ***No Information Without Legal Basis***: If you are unsure about the permissibility of providing information, ask the requesting party to disclose the legal basis for the request (e.g., a relevant legal provision or court order). If no clear legal basis is provided, refuse the request, citing data confidentiality. This applies even if the

requesting party is, for example, a government authority, as public offices and authorities are also bound by data protection laws.

- ***No Telephone Information***: Information provided over the phone is not permissible, unless you personally know the caller, as it is not possible to reliably verify the identity of the person on the other end (risk of misuse).
- ***Handling Particularly Urgent Requests***: Do not be pressured into providing immediate information by insistent requesters. Politely inform the requester that information cannot be provided without verifiable legitimacy (persistent pressure might be a deliberate tactic by the requester).
- ***Principle of Proportionality***: The information provided should be limited to what is absolutely necessary. Information that is not required for the requested disclosure should not be shared.

For further questions and to clarify any uncertainties or doubts, please feel free to contact our Data Protection Coordinator Alexander Gisy:

E-Mail: datenschutz@innofly.at
Phone: 0660 6233407

Data Breach Notification Procedure according to Article 33 of the GDPR

What must be reported?	Yes/No	
1. Data breach has been caused by a security deficit in the technical and organizational measures taken. **Examples**: unlawful data transfer to third parties, inadvertent incorrect addressing, sending emails to a large distribution list with "cc" and without "bcc" **Attention**! If the breach of the protection of personal data is not based on a deficit in the technical/organizational measures, then there is no reportable data breach.	**Yes** ☐	**No** ☐
1. The data breach has led to a. Destruction, b. loss, c. an alteration d. unauthorized disclosure, or e. unauthorized access to personal data. It is therefore a breach of confidentiality, integrity or availability.	**Yes** ☐	**No** ☐
2. The injury has objectively occurred. Suspicion alone is not sufficient. The obligation to notify exists if the data has been accessed, regardless of whether this is unintentional or intentional. It is not decisive whether the data was actually accessed. **Attention!** If we want to avoid a reporting obligation despite an existing security deficit, we must prove that the data has not been accessed.	**Yes** ☐	**No** ☐
3. Abolition of the obligation to notify those affected? Notification of the data subject is not required if the "high risk to the rights and freedoms of data subjects" no longer exists due to measures taken after the data breach (see Art. 34 (3) (b) GDPR). However, it should be noted that even if the data subject does not have to be notified for the above reasons, there is still an obligation to notify the data protection supervisory authority in accordance with Art. 33 GDPR! The risk is measured by the relationship between the severity of the potential damage and its probability of occurrence. The greater the damage to be assumed, the lower the probability requirements. **There is no obligation to report if:** - the data is publicly available anyway, - the data is effectively encrypted (unless there has been a permanent loss of data, e.g. because the only data carrier has been lost and there are no backups) - accidentally sending data to a trusted third party is a breach, but does not manifest a risk to the rights and freedoms of natural persons if a third party is bound to confidentiality as a professional secrecy holder and deletes or returns the data		

Assessment of the criteria **How high is the risk posed by the data breach?**	**High risk**	**Medium risk**	**Small risk**
Type of data breach (unauthorized access is often more serious than data loss)	☐	☐	☐

Identifiability (How easy and likely is it that a third party who gains unauthorized access can establish the personal reference?)	☐	☐	☐
Type and scope of data	☐	☐	☐
Number of people affected	☐	☐	☐
Special circumstances regarding the persons concerned (e.g. children, disabilities)	☐	☐	☐
Special circumstances regarding the person responsible (e.g. medical facility)	☐	☐	☐
Expected consequences: As regards the consequences, recital 85 lists typical groups of cases: - Loss of control over one's own data - Restriction of rights - discrimination - Identity theft or fraud - Financial losses - Cancellation of pseudonymization - Damage to reputation - Breach of professional secrecy - - Other significant economic or social disadvantages	**Assessment:**		

Documentation of the data breach (whether reportable or not)	**Done?**
1. timing of the data breach	☐
2. description of the data breach	☐
3. extent of the data breach	☐
4. consequences for affected persons	☐
5. measures to minimize the damage	☐
6. risk analysis	☐

Was the data breach reported?	**Done?**
The notification period begins to run from the time when anyone in the controller's company becomes aware of the significant facts of the data breach. This deadline also applies at weekends and even on public holidays such as Easter and Christmas. Vacation and illness are not taken into account when calculating the deadline.	☐ Date: Name: