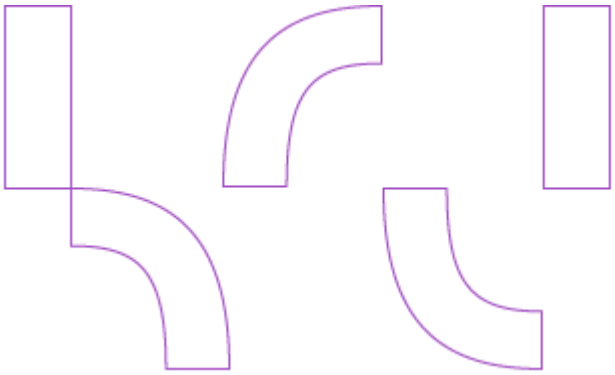
INNOFACTOR®



Privacy Policy

Policy

November 6, 2020

Confidential

This document contains business and trade secrets (essential information about Innofactor's business) and is therefore totally confidential. Confidentiality does not apply to pricing information.

Version History

Version	Date	Author	Description	Reviewed by	Approved by
1.0	27.2.2019	CSä	Initial version	APa	EB
1.1	6.11.2020	MSk	Updated DPO	MPa	MSk

Keilaranta 9
FI-02150 Espoo Finland

dpo@innofactor.com
www.innofactor.com

tel.: +358 10 272 9000
fax: +358 10 272 9001

Table of Contents

1 Introduction 1
2 Scope 2
3 Principles 3
4 Rights 5
5 Roles and responsibilities 7
6 Data breach investigation 9

Keilaranta 9
FI-02150 Espoo Finland
dpo@innofactor.com
www.innofactor.com
tel.: +358 10 272 9000
fax: +358 10 272 9001

1 Introduction

In accordance with our Code of Conduct, Innofactor respects the confidentiality and lawful processing of personal data. Innofactor recognizes the fundamental rights and freedoms of natural persons and their right to protection of personal data. Accordingly, Innofactor protects the privacy of its own employees and directors (hereinafter both jointly “employees”), customers, end-users, partners and their employees as well as other natural persons it has interactions with by implementing necessary technical and organizational measures to protect personal data.

The primary region where Innofactor operates consists of Finland, Sweden, Norway and Denmark and as EU privacy legislation is applicable in all these countries, also Innofactor applies this legislation and the applicable local laws to its operations, most notably the EU General Data Protection Regulation (“GDPR”). Innofactor’s central administration is in Finland.

Innofactor management is committed to the protection of personal data, and all Innofactor employees and contractors are required to protect personal data appropriately.

This policy describes the key principles and responsibilities for how we implement data protection at Innofactor. It is supported by our Information Security Policy and extended by further policies and guidelines.

2 Scope

This policy applies to all Innofactor companies and their employees, subcontractors, suppliers and other people working for Innofactor.

This policy applies to personal data about natural persons, as defined in the GDPR:

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); 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 person*

Innofactor processes personal data both in the role of the controller, for our own registers, and as a processor, for many of our customers.

3 Principles

We process personal data according to the following principles laid out by the GDPR, the national applicable laws implementing GDPR and other locally applicable legislation and mandatory regulations (hereinafter “the Laws”). We also follow the contractual commitments given for our customers in respect of processing any of their personal data.

3.1 Lawfulness, fairness and transparency

We ensure that personal data is only processed according to the Laws, we are fair against the persons whose data we process, and we are transparent about our processing.

We ensure that we inform persons about their rights and our processing of their personal data in a timely fashion, in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

3.2 Purpose limitation

We only process and allow the processing of the personal data that we control only for specified, explicit and legitimate purposes that have been duly identified.

3.3 Data minimization

We ensure that the personal data we process is adequate and relevant to the purpose and limited to only what is necessary for each purpose.

3.4 Accuracy

We make sure the personal data is accurate and we keep it up to date when necessary. Inaccurate data is corrected or deleted.

3.5 Storage limitation

We keep personal data in an identifiable form only for as long as necessary. After that, the data is either destroyed or permanently anonymized.

3.6 Security, integrity and confidentiality

We ensure the appropriate security of personal data, protecting it against unauthorized or unlawful processing and against accidental loss, destruction or damage – according

to our information security policy and our information security management system based upon ISO 27001.

3.7 Privacy by Design and Default

Before we begin processing personal data, we ensure that the rights of natural persons are implemented correctly, data protection principles are applied, and that suitable protections are in place to mitigate risks.

We ensure that, by default, only personal data which are necessary for each specific purpose are processed.

We take special care to ensure that personal data is not inadvertently exposed to the public.

3.8 Record of processing

We maintain a record of processing for each register of personal data where we are the controller, and for each service where we are a processor.

3.9 Controlled transfer of data

We do not transfer personal data outside of Innofactor, or outside of the European Economic Area (EEA) without suitable contractual safeguards. We respect our contractual duties to ask approvals of the transfer of personal data outside Finland / EU if so agreed in our customer contracts.

4 Rights

We implement the rights of natural persons according to the GDPR.

Where Innofactor is the processor of personal data on behalf of a customer, we assist the customer as the controller in implementing these rights. We, however, shall be clear, when entering into our contacts, on what extent such assistance is chargeable and to what extent it is included in the service provided in order to avoid any disputes with the customer.

4.1 Right to be informed

We provide information regarding personal data processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular if addressing a child.

We inform persons about their rights. We have published privacy statements on our web pages and intranet on how we process personal data.

4.2 Right of access and data portability

We give people access to their own personal data and the purposes for which we process the data.

We provide people a copy of their own data within the timeframes set forth in the Laws, as long as this does not affect the rights of others – including our customers and Innofactor itself.

4.3 Right to rectification and notification

We provide people the opportunity to correct or complete their personal data, and to the best of our abilities we also propagate any changes to whoever might have received copies of the data.

4.4 Right to be forgotten

We respect the right of a person to be forgotten once data is no longer needed and recognize that sometimes we are under an obligation to keep some data safe for a long time.

4.5 Right to restriction of processing

We implement the ability to freeze personal data processing under certain conditions.

4.6 Right to object

We support the right to object to processing when we process data based upon our own legitimate interest, some official authority or public interest. This includes the right to opt out of direct marketing.

4.7 Right not to be subject to automatic decision-making

We respect a person's right not to be subject to an automated decision or profiling that produces legal effects on them or otherwise significantly affects them. If such decision-making is necessary, we ensure we ask for consent or ensure that the person has the right to ask for a review of the decision.

4.8 Right to file a complaint

We inform persons about their right to file a complaint about how we process their personal data.

5 Roles and responsibilities

5.1 Risks

This policy helps to protect Innofactor from some very real personal data risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how we use data relating to them.
- Reputational damage. For instance, we could suffer if hackers successfully gained access to sensitive data.
- Possible sanctions laid by the Laws.
- Possible breaches of commitments given to our customers that can in the worst cases lead to premature termination of our agreements and to duty to pay damages.

Considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of registered persons, we implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

We review and update the protections when necessary.

5.2 Controller

For the registers maintained by Innofactor, a responsible employee is designated Controller of the register.

The Controller is responsible for implementing appropriate technical and organizational steps to protect personal data.

5.3 Processor

Where we carry out processing of personal data on behalf of our customer, a responsible contact is designated for our role as Processor.

We provide customers guarantees that we implement appropriate technical and organizational measures to meet legal requirements and to ensure the protection of the rights of the registered persons. We only use sub-processors as agreed with the customer and ensure sub-processors also meet the obligations. We make sure that our subcontracting agreements are in line with the customer requirements; special attention shall be paid to audit rights, transfer of personal data outside EEA and to clauses requiring approval for the use of subcontractors.

We only process personal data under a suitable written contract and documented instructions from the Controller, unless required by law, and ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.4 Responsibilities

5.4.1 Board of directors

The board of directors is ultimately responsible for ensuring that Innofactor meets its legal obligations.

5.4.2 Employees and contractors

Any person acting under the authority of the Controller or of the Processor, who has access to personal data, must not process those data except on instructions from the Controller, unless required to do so by Union or Member State law.

In addition, each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

Where no more specific instructions exist, our general Personal Data Handling instruction must be followed. The instruction is available in 100%Quality.

5.4.3 Data Protection Officer

Innofactor carries out processing on behalf of public authorities and bodies and has designated a Data Protection Officer (DPO) for the whole Innofactor Group.

The DPO's tasks are

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations;
- to monitor compliance with data protection regulations and this policy, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested regarding data protection impact assessment and monitor its performance;
- to cooperate with the supervisory authority;
- to act as the contact point for the supervisory authority;
- to coordinate responses to requests for personal data, also known as 'subject access requests'.

The DPO is Michaela Skrabb <dpo@innofactor.com>.

6 Data breach investigation

Suspected personal data breaches must be investigated immediately, to enable us to notify affected customers, persons, and data protection authorities in the required timeframe.

Anyone suspecting a data breach must immediately report it internally according to our guidelines on reporting security incidents.