

# Privacy Statement

For External Parties

## TABLE OF CONTENTS

DEFINITIONS AND ABBREVIATIONS .....	3
INTRODUCTION .....	4
THE PURPOSE OF PROSECCING PERSONAL DATA.....	5
PERSONAL DATA PROCESSED .....	5
MARKETING.....	5
DISCLOSURE OF PERSONAL DATA.....	6
TRANSFER AND DISCLOSURE OF PERSONAL DATA .....	6
NOTIFICATION AND CONSENT .....	6
PROTECTION OF YOUR PERSONAL DATA .....	7
PERSONAL DATA RETENTION .....	7
UPDATE OF PERSONAL DATA.....	7
ACCESS, CORRECTIONS AND DELETING PERSONAL DATA.....	7
INQUIRIES OR CONCERNS.....	7
REVISIONS TO THIS PRIVACY STATEMENT .....	8

## DEFINITIONS AND ABBREVIATIONS

<b>Term</b>	<b>Definition</b>
<b>Personal data</b>	Personal Data is any information related to a person that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address. Personal Data does not include anonymous or non-personal information (i.e., information that cannot be associated with or tracked back to a specific individual).
<b>Legal basis</b>	A legal basis for processing personal data. The most relevant bases are a law, an agreement, consent, or a legitimate interest.
<b>Legitimate interest</b>	Legitimate interest can be used as a basis for processing personal data. It is relevant to consider whether legitimate interest can be used as the legal basis if the business cannot obtain valid consent, has statutory authority, or processes personal data based on contractual terms. A business can process personal data if it is necessary to safeguard a legitimate interest that outweighs the individual's privacy interests. This means choosing the least invasive processing method.
<b>Consent</b>	A voluntary, explicit, and informed declaration by the data subject that they accept the processing of their personal data.
<b>Processing</b>	Any handling of personal data, such as collection, registration, organization, structuring, storage, adaptation or modification, retrieval, consultation, use, disclosure, dissemination, compilation or merging, restriction, deletion, or destruction.
<b>Controller</b>	The entity that determines the purpose of processing personal data and the means to be used. CEO serves as the controller at InflowControl and has, together with the Board of Directors the responsibility for processing personal data in InflowControl.
<b>Processor</b>	The entity that processes personal data on behalf of the controller.
<b>Data Subject</b>	The person to whom the personal data can be related
<b>GDPR</b>	General Data Protection Regulation
<b>DPA</b>	Data Processing Agreement. An agreement between the data processor and the data controller (or between the data processor and another data processor) on how personal data should be handled.

## INTRODUCTION

This Privacy Statement provides information about what personal data InflowControl process about their external stakeholders, what the data is used for, how it is processed and to whom such data is disclosed.

This statement applies to the Personal Data of all individuals that is either a Customer, an employee of a Customer, a Supplier or an employee of a Supplier or individuals registering their personal data on [www.inflowcontrol.no](http://www.inflowcontrol.no), the Data Subject.

The Privacy Statement also informs Data Subjects of their rights related to protection of Personal Data.

## THE PURPOSE OF PROSECCING PERSONAL DATA

Personal Data of Data Subjects, shall be collected, used or otherwise Processed for one (or more) of the following Business Purposes:

- Providing, development and improvement of products and/or services purposes.
- Conclusion and execution of agreements with Customers, Suppliers and Business Partners
- Relationship management and marketing purposes. This includes activities such as maintaining and promoting contact with Customers, Suppliers and Business Partners, account management, customer service, recalls and the development, execution, and analysis of market surveys and marketing strategies
- Business process execution, internal management, and management reporting purposes
- Health, safety and security purposes
- To comply with legal obligations
- To protect vital interests of Employees or Data Subjects
- Cookies

## PERSONAL DATA PROCESSED

InflowControl collects and maintains different types of Personal Data in respect of Data Subjects. This includes e.g. the Personal Data contained in:

- Contact information such as name and address, telephone numbers and email address
- Business details, including the names of relevant office holders of a company and business numbers
- Where permitted or required by applicable law or regulatory requirements, InflowControl may collect information about individuals without their knowledge or consent

## MARKETING

Contact information from visitor's PDF downloads may be used to inform and promote products and/or services by e-newsletter or email. If such information is chosen for promotion, unsubscribing from the newsletter will be available at any time. This contact information will not be disclosed to any other third parties outside of InflowControl and is safely stored in the CRM system.

Cookies are used on the website to make it easier to use web pages and can be used to personalize certain parts of the content. A cookie is a small text file sent from a web server and stored by the browser. The information stored may be information about how users have surfed and used web pages and what browser they have used. Statistics about users and traffic / traffic providers are used in aggregated form. The statistics never contain any kind of personal information, everything is anonymous. IP addresses are not stored in the database where site behavior is stored, so information about users can never be linked to their identity. IP addresses are stored for security reasons only in cases where users actively register on the site.

## DISCLOSURE OF PERSONAL DATA

Personal Data may be shared with employees, contractors, consultants, and other parties (including other members of the InflowControl group) who require such information to assist fulfilling the business purposes of InflowControl. This includes parties that provide products or services to or on behalf of InflowControl. In some instances, such parties may also provide certain information technology and data processing services to enable business operations. Personal Data may be shared with such parties both in and outside of the home jurisdiction, and as a result, Personal Data may be collected, used, processed, stored, or disclosed in Norway or any other country where InflowControl is present.

## TRANSFER AND DISCLOSURE OF PERSONAL DATA

Personal Data is only transferred to external parties, outside the InflowControl Group if this is required or permitted under the applicable privacy legislation. When Personal Data is shared with external parties, the external party must enter into a Data Processing Agreement (DPA) with InflowControl in compliance with the GDPR. Such parties may only use or disclose Personal Data in a manner consistent with the use and disclosure provisions of this Privacy Statement. Further, Personal Data may be disclosed in the following situations:

- If permitted or required by applicable law or regulatory requirements. In such a case, we will endeavour to not disclose more Personal Data than is required under the circumstances.
- To comply with valid legal processes such as search warrants, subpoenas, or court orders; or
- As part of InflowControl's regular reporting activities to other members of the InflowControl group (including outside of your home jurisdiction); or
- As part of transactions or divestments which involves third parties. In such a case, we will endeavour to not disclose more Personal Data than is required under the circumstances.
- To protect the rights and property of InflowControl;
- During emergency situations or where necessary to protect the safety of a person or group of persons;
- Where the Personal Data is publicly available; or
- With consent where such consent is required by law.

## NOTIFICATION AND CONSENT

Privacy laws do not generally require obtaining consent for the collection, use or disclosure of Personal Data for the purpose of conducting business purposes of InflowControl. In addition, Personal Data may be collected, used, or disclosed without knowledge or consent were permitted or required by applicable law or regulatory requirements to do so. In some situations, however, consent might be required for the collection, use or disclosure of Personal Data. In such cases consent may be withdrawn at any time, subject to legal or contractual restrictions and reasonable Statement. To withdraw consent, please send an email to the contact person in InflowControl.

## PROTECTION OF YOUR PERSONAL DATA

InflowControl endeavours to maintain physical, technical, and procedural safeguards that are appropriate to the sensitivity of the Personal Data in question. These safeguards are designed to protect Personal Data from loss and unauthorised access, copying, use, modification, or disclosure.

## PERSONAL DATA RETENTION

Except as otherwise permitted or required by laws or regulations, InflowControl endeavours to retain Personal Data only for as long as necessary to fulfil the purposes for which the Personal Data was collected. Instead of destroying or erasing Personal Data, it may be anonymized so that it cannot be associated with or tracked back to individuals.

## UPDATE OF PERSONAL DATA

It is important that the Personal Data in records is both accurate and current. If Personal Data happens to change, please inform the organization of such changes.

## ACCESS, CORRECTIONS AND DELETING PERSONAL DATA

Individuals have the right to access information about Personal Data. To review, verify, correct or delete Personal Data, an email should be sent to the contact at InflowControl. Necessary steps will be taken to confirm the data subject's identity before providing any information regarding personal data. The request will, when the requestor's identity is confirmed, be answered within 30 days. In some instances, the request may take longer, but notification will be provided accordingly and an answer sent at the latest within 90 days.

The right to access Personal Data is not absolute. There are instances where law or regulations allow or require refusing to provide some of the Personal Data. There may also be statutory requirements preventing deletion of some Personal Data. In the event that a request cannot be fulfilled, information about the reasons will be provided, subject to any legal or regulatory restrictions.

## INQUIRIES OR CONCERNS

For questions about this Privacy Statement, concerns about Personal Data management, or to file a complaint, please contact the CFO. Questions will be answered and steps taken to address issues at earliest convenience and at the latest within one month after the request is made.

To file a complaint regarding compliance with this Privacy Statement or violations of rights, complaints may be sent to the CFO or to Datatilsynet.

## REVISIONS TO THIS PRIVACY STATEMENT

InflowControl may from time to time make changes to this Privacy Statement to reflect changes in legal obligations or in the manner of dealing with Personal Data. A revised version of this Privacy Statement will be communicated. The at all times applicable and updated Data Protection Statement is available on [www.inflowcontrol.com](http://www.inflowcontrol.com). Any changes to this Privacy Statement will be effective from the time they are communicated. Any change that relates to collection, use or disclose your Personal Data, require consent, this will not apply until consent have been obtained.