

Privacy and Data Protection Policy

Ver. 002.O1

Opscom Systems as

Olav V. gate 56-60
8004 Bodø
Norway

Contents

1 Scope 4

2 What is personal data and data protection? 4

2.1 Which data protection regulation is applicable? 4
2.2 What is personal data? 4
2.3 What does processing of personal data mean? 5
2.4 Controller vs. processor 5

3 What are the basic principles of data protection? 6

3.1 Lawfulness 6
3.2 Fairness 6
3.3 Transparency 6
3.4 Confidentiality and integrity 7

4 What personal data do we process? 7

4.1 The data you actively and knowingly provide us 7
4.2 The data you provide to us by the use of our service 7
4.3 Who are registered? 7

5 Why do we process your personal data? 7

5.1 Proportionate processing 7
5.2 Processing activities 8

6 How do we process your personal data? 8

6.1 Principles 8
6.2 Technical and organizational measures 9

7 Your rights as a data subject 9

7.1 Right of access 9
7.2 Right to rectification 10
7.3 Right to be forgotten 10
7.4 Right to the restriction of processing 10
7.5 Right to data portability 11
7.6 Right to object 11
7.7 Automated individual decision-making 11
7.8 The right to withdraw consent 12
7.9 Procedure for exercising your rights 12

7.10 Right to lodge a complaint with the supervisory authority 12

8 Do we share your personal data? 13

8.1 Transfer to third countries 13

9 Website and apps 14

10 Cookies 14

10.1 What are cookies? 14

10.2 Categories of used cookies 14

11 More information and Data Protection Officer 14

12 Audit and review 15

13 Entry into force 15

14 Policy duration 15

1 Scope

Your privacy is very important to us. Opscom Systems therefor carefully considers the protection of your personal data during the different personal data processing activities.

This policy aims to tell you which personal data we collect from you, why we collect this data and how your data will be used. In addition, you can find information about your rights as a Data Subject.

2 What is personal data and data protection?

The applicable data protection legislation uses specific language and in order to help you to better understand the terminology and this policy, we will explain the most important elements below. If you want more information, you can check out the website of the European Commission at

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens_en

2.1 Which data protection regulation is applicable?

The basic principles and obligations are documented in the General Data Protection Regulation (GDPR or in legalese Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data). Next, the Privacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector) is applicable in specific cases, such as the use of cookies.

In addition to the European regulations, the national data protection legislation still applies to the processing of your personal data.

2.2 What is personal data?

Personal data is all the information about an identified or identifiable natural person, also known as the data subject (a.k.a. you). A person is considered ‘identifiable’ when a natural person can be directly or indirectly identified, in particular by reference to an identifier such as:

- a name;
- an identification number;
- location data;
- an online identifier;
  or one or more elements that are characteristic of the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person (article 4, §1 GDPR).

Data relating to race or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and processing of genetic data, biometric data for the unique identification of a person, or data about health, sexual behaviour or sexual orientation, criminal offences or convictions are considered sensitive data. Unless an organization can refer to one of the exceptions, the processing of these data is forbidden pursuant article 9 of the GDPR.

We at Opscom Systems do process sensitive personal data, but only in the capacity as processor.

2.3 What does processing of personal data mean?

This means any operation or set of operations which is performed on personal data (whether or not by automatic means), such as the:

- collection, recording, organization, storage, consultation, use, etc (art.4, §2 GDPR)

2.4 Controller vs. processor

The controller is a natural or legal person that determines the purposes and means for the processing of personal data. In our context, the controller is the owner of the site and the data connected to this unique site.

The processor on the other hand, processes this data on behalf of and only on request and with instructions from the controller (art. 4, §7 and §8 GDPR).

Opscom Systems as controller	Opscom Systems as processor
for the processing of data in the context of: • the Opscom Systems App • the Opscom Systems website In this context the customer is the data controller on all Opscom customer sites.	Opscom Systems work with several Airports, Air Operators, ATC organizations, 145 stakeholders and other entities within Police, Military and Shipping. Each customer has a unique database, accessed through their own secure log on. Their employees have access to this database, based on their user rights.

3 What are the basic principles of data protection?

3.1 Lawfulness

Personal data must be processed fairly and lawfully with respect to you. In order to process personal data lawfully, a legal basis must exist.

Pursuant article 6 of the GDPR, these legal bases are:

- consent;
- performance and preparation of a contract;
- compliance with a legal obligation;
- protection of vital interests;
- performance of a task carried out in the public interest or in the exercise of official authority;
- legitimate interest.

Opscom Systems ensures that it always refers to at least one of the above-mentioned legal bases when it processes personal data. More about our processing activities and their legal ground can be found below.

3.2 Fairness

The fairness of processing obliges us to only process your accurate (updated) data for specific, explicit and legitimate purposes. Processing incompatible with the initial purpose for which the data were collected, is not allowed.

Data minimization is also a key principle and limits the processing to what is necessary for the purposes for which the data were collected. This also implies the processing must be limited in time.

3.3 Transparency

You as a data subject must be made aware of the following matters in clear and plain language:

- Identity and contact details of the controller.
- If a Data Protection Officer is appointed all contact details.
- Processing purposes and legal basis.
- If the personal data processing is supported by a legitimate interest and an explanation of this interest.
- Categories of receivers of the personal data.
- Transfer of personal data to third countries (outside the EU) or international organizations (and on what basis)
- Time limit for the storage of personal data or the criteria used to determine the time limit.

- Your rights (including the right to revoke consent);
- The right to lodge a complaint with the supervisory authority;
- Explanation when the transmission of personal data is a contractual or legal obligation;
- If the personal data is received from a third party, the categories of personal data received and identification of the third party.

Specific legislation may contain exceptions or set additional requirements which the organization must comply with, with respect to the provision of information to data subjects. These mandatory legal provisions take precedence over this policy.

3.4 Confidentiality and integrity

Technical and organizational measures must be taken to ensure the processing of personal data can take place with the appropriate guarantees, so that the data are protected against accidental loss and against unlawful processing, destruction or damage.

4 What personal data do we process?

4.1 The data you actively and knowingly provide us

In principle we at Opscom Systems only process data we have received directly from you or from your employer in their daily use of the designated Opscom site.

4.2 The data you provide to us by the use of our service

You might not be aware of it but by using the designated Opscom site, you provide us with some data that might be personal (‘Observed data’), such as IP address, metadata (data that provides information about other data) and login time.

4.3 Who are registered?

Data Subjects affected by this DPP (Data Protection Policy) are users defined by the Data Controller.

5 Why do we process your personal data?

5.1 Proportionate processing

Opscom Systems only processes personal data if necessary to achieve a certain objective. That is why we use your personal data when necessary for:

- The compliance with a legal obligation which is imposed upon the organization;
- The purposes of the legitimate interests of our company in conducting and managing our business to enable us to give you the best service/products and the best and most secure experience.

Otherwise, we will make sure to obtain your explicit consent.

If you have given your consent for a specific processing purpose to Opscom Systems in order to process your data for that purpose, you can withdraw this consent at any time. We will then stop any further processing of your data for which you gave consent and will inform you of the possible consequences of your withdrawal of consent. If Opscom Systems processes your personal data for other purposes and in order to do so it refers to other legal bases, we will still be allowed to process your personal data.

5.2 Processing activities

Opscom Systems tries via its current privacy and data protection policy to provide you with this information in order to be as transparent as possible with respect to the processing of your personal data. This general policy must be read together with more specific

information notes which give additional information concerning about the organization's specific processing purposes.

We process your personal data for the following:

- To enhance security
  We may use your personal data to enhance the security of our networks and information systems based on our legitimate interest. This means we can monitor your access to our networks and systems and collect some metadata.
- To improve our products
  In order for Opscom Systems to improve our products and to understand how people interact with them, we may process your data on the use of our products based on our legitimate interest. For example, we collect data on how many times you have accessed your account.

If we wish to use your data for statistics, we will anonymize this data first.

6 How do we process your personal data?

6.1 Principles

We at Opscom Systems ensure that your personal data shall be processed

- For specific, explicit and legitimate purposes and may not be processed further in a way incompatible with the initial purposes for which the data were collected. Therefore, we shall clearly communicate the purposes before starting the processing.
- Limited to what is necessary for the purposes for which the data were collected. If possible, Opscom Systems will anonymize the data or use pseudonyms in order to limit the impact for the data subject as much as possible.
- Limited in time and only as necessary for the specific purpose.
- Opscom Systems has defined a retention policy based on current legal requirements from EASA.

- Accurately, and the data shall be updated when necessary. Opscom Systems shall take all reasonable measures to erase or update the personal data, taking into account the purposes for which they are processed.
- Transparently, therefore Opscom Systems shall provide you the required information in a clear and plain language. Depending on the concrete case, we can disclose the information both on a collective and/or individual basis.

6.2 Technical and organizational measures

Opscom Systems is committed to keeping your information as secure as possible. Therefor we have implemented various technical and organizational measures (art. 25, §2 GDPR) to protect your personal data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, etc. We have, when choosing the proper security measures, considered the nature, context, purpose and scope of the processing, the possible risks when processing the personal data, the costs for the implementation of the measures and the state of the art. It is however important to remember that the internet is an open system and we cannot guarantee that unauthorized third parties will never be able to defeat those measures or use your personal data for improper purposes. Nevertheless, we at Opscom Systems commit ourselves to keep updating and reviewing these measures so that we can offer your personal data an appropriate safety level.

You can help us with this by regularly updating the Opscom Systems APP, as well as other software installed on your devices.

These measures are applicable to the physical access to personal data, access to the personal data via computers, servers, networks or other IT hardware and software applications and databases. Examples of these measures include but are not limited to: the appointment of a Data Protection Officer, Data protection policy and management, retention policy, incident response plan, processor management, regular evaluations of policies, storage of data in controlled facilities with limited access (by e.g. physical access control), confidentiality obligations and awareness trainings for employees, role-based access control systems.

The organization shall ensure that the third parties that receive personal data from the organization will comply with the applicable data protection legislation and this policy.

7 Your rights as a data subject

Opscom Systems adheres great importance to your privacy rights and therefor complies with reasonable effort with these rights, considering the legal limitations in exercising them.

7.1 Right of access

Pursuant article 15 of the GDPR, you have the right to obtain confirmation from the organization of whether or not your personal data are being processed. If your data are being

processed, you may request the right to consult your personal data as used/stored by the organization.

Opscom Systems shall inform the data subject about the following:

- the processing purposes;
- the categories of personal data concerned;
- the receivers or categories of receivers to which the personal data are supplied;
- transfer to receivers in third countries or international organizations;
- if possible, the period during which it is expected that the personal data will be retained, or if this is not possible, the criteria used to determine this period;
- that the data subject has the right to ask the organization to correct or erase personal data, or to limit the processing of his or her personal data, as well as the right to object to this processing;
- that the data subject has the right to lodge a complaint with a supervisory authority;
- if the personal data are not collected from the data subject, all available information about the source of the data;
- the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Opscom Systems shall also supply a copy of the relevant personal data that are being processed. For any further copies requested by the data subject, the processor may charge a reasonable fee.

7.2 Right to rectification

When you establish that Opscom Systems has incorrect or incomplete data about you, you always have the right to inform us of this fact so that appropriate action can be taken to rectify or supplement these data. It is the data subject's responsibility to provide correct personal data to the organisation (article 16 GDPR)

7.3 Right to be forgotten

You as a data subject can ask to have your personal data erased pursuant article 17 of the GDPR if the processing of this data is not in accordance with the data protection legislation and within the limits of the law.

7.4 Right to the restriction of processing

You may ask to have the processing restricted (article 18 GDPR) if:

- The accuracy of the personal data is contested by the data subject, for a period enabling the controller to check their accuracy;
- The processing is unlawful and you oppose the erasure of the data;
- The organization no longer needs the data, but you request that your data are not be removed, given that you might need them for the exercise or defense of legal claims;

- You have objected to processing, pending the verification whether the legitimate grounds of the controller override those of the data subject.

7.5 Right to data portability

You have the right to obtain your personal data which you provided to the organization in a structured, commonly-used and machine-readable format pursuant article 20 of the GDPR. You have the right to have those personal data transmitted to another controller (directly by the organization).

This is possible if you have consented to the processing and if the processing is carried out via an automated process.

7.6 Right to object

When personal data are processed for direct marketing purposes (including profiling), you can always object to this processing.

You can also object to processing due to a specific situation regarding yourself as the data subject. Opscom Systems shall stop processing the personal data unless we demonstrate compelling legitimate grounds for the processing which overrides the interests of the data subject or for the exercise or defence of legal claims (article 21 GDPR).

7.7 Automated individual decision-making

Since Opscom Systems does not make automated individual decisions, this paragraph is only meant to inform data subjects of the full range of actions that can be taken under article 22 of the GDPR.

You as a data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you such as by evaluating personal aspects with respect to the performance of work, reliability, creditworthiness, etc.

This right not to be subjected to such automated decision-making does not exist when the decision is permitted by a mandatory legal provision.

Nor may you invoke this right when the decision is necessary for entering into, or the performance of, a contract between the data subject and the organization or is based on the data subject's explicit consent. In these last two cases, you do have the right to obtain human intervention from someone at the organization and you have the right to make your point of view known and to challenge the automated decision process.

7.8 The right to withdraw consent

If you have given your consent for a specific processing purpose to Opscom Systems in order to process your data, you can withdraw this consent at any time by adjusting your privacy settings or by sending an e-mail to: support@opscomsystems.com

7.9 Procedure for exercising your rights

You may exercise your rights by:

- Adjusting your privacy settings in the app or on the website; or
- Sending an e-mail to the Data Protection Officer via support@opscomsystems.com

Since we want to make sure you are really you, we can ask you to identify yourself. That way we can ensure that it is indeed the data subject requesting to exercise his or her rights.

If you have any questions about the application of the principles or the organization's (legal) obligations, you can always contact the Data Protection Officer via support@opscomsystems.com

In principle Opscom Systems shall respond to the data subject's request within one month. If not, we shall inform you why the request received no response or why it did not receive a response in good time. Opscom Systems shall take the necessary measures to inform the receivers of the data subject's personal data about exercising the right to correction, right to erasure or the limitation of processing by the data subject.

Exercising your rights is in principle free, but in the event you exercise of multiple and/or unreasonable requests, we can ask a reasonable fee.

7.10 Right to lodge a complaint with the supervisory authority

You have the right to lodge a complaint with the competent supervisory (data protection) authority. If you like to log a complain on behalf of a company, use the web address. This will lead you to Altinn as the Norwegian reporting interface.

Norwegian Data Protection Authority (Datatilsynet)

Postboks 458 Sentrum,
0105 Oslo, Norway
Tel: 22 39 69 00

https://www.altinn.no/skjemaoversikt/datatilsynet/melding-om-avvik-datatilsynet

You can also report/make a complaint outside Altinn, by sending a standard form to:

postkasse@datatilsynet.no

Please fill in all relevant fields (1-9)

https://www.datatilsynet.no/regelverk-og-skjema/avviksbehandling/melde-avvik-til- datatilsynet

8 Do we share your personal data?

In some cases, it may be necessary to transfer your personal data to third party receivers. This will only be done if your company is participating in a safety related study or safety related research.

We can share your personal data, based on our legitimate interest, to third party providers who help us with our products and services. Examples include third parties hosting our web servers, providing marketing assistance, and providing customer service. These processors will have access to your personal data but only when strictly necessary to perform their functions on instructions from Opscom Systems and they may not use that data for any other purpose. Our Processor Management implies that we make sure these processors also comply with the legal requirements pursuant data protection legislation and observe the necessary security measures when transferring the data and with respect to the receivers, in order to guarantee the confidentiality and integrity of the personal data. Processing agreements containing obligatory clauses are conducted with our processors.

We may disclose your personal data to enforce our policies, to comply with our legal obligations or in the interests of security, public interest or law enforcement in any country where we have entities or affiliates. For example, we may respond to a request by a law enforcement agency or regulatory or governmental authority. We may also disclose data in connection with actual or proposed litigation, or to protect our property, security, people and other rights or interests.

In the event that the business of Opscom Systems is sold or integrated with another business, your details will be disclosed to any prospective purchaser's adviser and will be transferred to the new owners of the business. In this case, we will implement the appropriate safeguards to ensure the integrity and confidentiality of your personal data. However, use of your personal information will remain subject to this Policy.

8.1 Transfer to third countries

It is also possible for the organization to transfer your personal data to parties (processors) that are based in third countries, these are countries outside the European Economic Area (i.e. The European Union, Norway, Iceland and Liechtenstein).

Such a transfer is possible if the country where the receiver offers sufficient legal guarantees to protect your personal data and which the European Commission has assessed as being adequate. In other cases, the organization has concluded a standard contract with

the receiver so that equivalent or similar protection to that offered in Europe is offered. Opscom Systems ensures to have such safeguards in place when transferring your data to third countries.

9 Website and apps

We use cookies to process data such as your IP address, the type and language of your browser, the brand and type of equipment you are using, the time and duration of our website/app use, the webpage from which you reached our website, the actions you undertake such as clicking on links and so on. We use these data to improve and personalize our products, services and website, to provide services, to communicate with you and to provide you with information based on our legitimate interests.

We monitor traffic patterns on the website and gather broad demographic information for aggregate use to analyse trends and administer the website. This enables us to improve its layout and design and permits for website personalization and streamlining to create the best experience we can for our users. In order to perform analysis permitting such personalization and improvement of site design and user experience, we may employ suitable third parties with whom we share the information necessary to accomplish these objectives. Where appropriate, we share aggregated statistical information with our business partners. These statistics, however, include no personally identifying information.

10 Cookies

10.1 What are cookies?

Cookies are text files which contain small pieces of information, sent by a web server to a web browser which allows the server to store different types of information on the web browser's device. They will be stored on your computer, tablet or phone when you visit a website. Cookies may contain identifying information.

Opscom requires the use of Strictly Necessary Cookies to give you access to the Opscom site. If you choose to reject these cookies, the Opscom site will not allow you access.

10.2 Categories of used cookies

We use the following categories of cookies on our website:

- Strictly Necessary Cookies:
  - These cookies are essential in order to help you to move around the website and use its features. Without these cookies, services you have asked for such as remembering your login details cannot be provided.

11 More information and Data Protection Officer

Opscom Systems has not appointed a Data Protection Officer ('DPO'). Opscom does not process largescale sensitive personal information.

The responsibilities defined to the role DPO are in Opscom Systems handled by our Chief Information Security Officer (CISO). Our CISO is independent in the performance of his or her tasks with respect to the protection of personal data. This means that he or she is not bound by instructions from managers in the performance of his or her tasks. Our CISO will, in addition to advising the company, also supervise the company's compliance with data protection legislation, this policy and any other related policies.

If you wish to obtain more information regarding the processing of your personal data or your rights, please contact our CISO.

Opscom Systems AS
Att: CISO

E-mail: post@opscomsystems.com
Telephone: +47 47 77 55 10

12 Audit and review

The organization reserves the right to adjust and review this policy when it deems necessary and to remain coherent with the legal obligations and/or recommendations of the competent supervisory authority for data protection.

The organization shall inform the data subject when it is impossible for it to comply with this policy due to mandatory legal provisions which are imposed upon the organization.

13 Entry into force

This policy applies as of May 25th, 2018.

14 Policy duration

This policy is in effect until one of the parties terminates the agreement.

All personal data will be deleted or transferred in agreement with the Data Controller.