Stavanger Barnevaktbyrå's Data protection policy

Goal of our data protection policy

This document outlines our data protection policy in line with the European General Data Protection Regulation (GDPR).

1. Introduction

1.1 The General Data Protection Regulation (GDPR) protects the 'rights and freedoms' of a living nature person in regard to their personal data, its processing and storage.
1.2 Some definitions used in this document are taken directly from the GDPR:

> **Personal data** -- any information relating to an identified or identifiable living natural person either directly or indirectly related, such as name, ID numbers, location coordinates, etc. or characteristics like physical, mental, cultural descriptions and so on.
>
> **Data controller** -- responsible party, either jointly or alone, involved in determining the purposes for having and processing personal data.
>
> **Data subject** -- any living nature person whose personal data is obtained by a data controller.

2. Policy statement

2.1 The employers of Stavanger Barnevaktbyrå are committed to complying with all relevant laws in accordance with the GDPR.

2.2 Compliance with the GDPR is described within the sections of this policy along with associated processes and procedures.

2.3 The GDPR and this policy apply to all of Stavanger Barnevaktbyrå's personal data processing functions, including those performed on customers, clients, employees, suppliers and partners and any other personal data the organization processes from any source.

2.4 Stavanger Barnevaktbyrå has established objectives for data protection and privacy which are detailed in the sections below.

2.5 Stavanger Barnevaktbyrå's Data Protect Officer (DPO) is responsible for any changes to Stavanger Barnevaktbyrå's activities related to its data protection practices.

> **Current DPO as of 18th of August 2017**: Inger Lise Strand
>
> **Contact Email**: post@stavangerbarnevakt.no

2.6 This policy applies to all Employees/Staff and outsourced suppliers. Any breach of this policy will be dealt with by Stavanger Barnevaktbyrå's DPO, and in cases where the matter is criminal, the appropriate authorities will be notified.

2.7 Any third parties working with or on behalf of Stavanger Barnevaktbyrå, and who have access to personal data, will be expected to have read, understood and to comply with this Data Protection Policy.

3. Roles and responsibilities

3.1 Stavanger Barnevaktbyrå is a data controller and/or data processor under the GDPR.

3.2 Top Management and all those in managerial or supervisory roles throughout Stavanger Barnevaktbyrå are responsible for developing best practices within Stavanger Barnevaktbyrå regarding data protection.

3.3 Our DPO is also our CEO, and is accountable for the management of personal data within Stavanger Barnevaktbyrå and for ensuring Stavanger Barnevaktbyrå compliance with data protection laws and best practices which includes:

3.3.1 development and implementation of the GDPR

3.3.2 Security and risk management as it applies to the GDPR.

3.4 Our DPO has a daily responsibility for Stavanger Barnevaktbyrå compliance with the GDPR in relation to the personal data processing that takes place within their area of responsibility.

3.5 Our DPO has the duty to perform procedures such as Right to be Forgotten as well our staff's primary contact for help in any areas related to data protection compliance.

3.6 Compliance with the GDPR is the responsibility of all employers of Stavanger Barnevaktbyrå.

3.7 Stavanger Barnevaktbyrå Staff is subject to periodic training in matters relating to data processing.

3.8 Staff have the obligation to provide Stavanger Barnevaktbyrå accurate and up-to-date personal information about themselves.

4. Policies and Procedures

4.1 Stavanger Barnevaktbyrå policies and procedures are designed for compliance with the guidelines of Article 5 of the GDPR, in short to process personal data lawfully, fairly and transparently. Where applicable, to provide the data subject a minimum of information which includes:

4.1.1 the identity and the contact details of the controller (i.e. Stavanger Barnevaktbyrå) ;

4.1.2 the contact details of our DPO;

4.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

4.1.4 the period for which the personal data will be stored;

4.1.5 the data subject's rights to request the following: access or deletion of his/her personal data, the correction errors within their personal data, a review of the process or procedure for collection and storage.

4.1.6 The intention to transfer personal data to a recipient in a third country (i.e. non-European country).

4.2 Personal data can only be collected for specific and legitimate purposes and will not be used for purposes other than stated.

4.3 Personal data must be restricted to what is necessary for processing

4.3.1 Our DPO is responsible for ensuring that Stavanger Barnevaktbyrå does not collect unnecessary personal data information.

4.3.2 All our data collection forms have a link to our privacy statement.

4.3.3 At least, once a year our DPO perform Data Protection Impact Assessments (DPIAs) on our processes to ensure compliance.

4.4 Personal data maintenance considerations:

4.4.1 Personal data is stored only if it's presumed accurate.

4.4.2 Staff are trained in collecting accurate personal data.

4.4.3 The data subject is responsible for providing accurate and up-to-date personal data upon completion of any Stavanger Barnevaktbyrå submission form.

4.4.4 A person aware of a change in circumstance related to Stavanger Barnevaktbyrå's accurate storage of personal data ought to notify Stavanger Barnevaktbyrå so that the change of circumstances is recorded and acted upon.

4.4.5 Our DPO responds to requests from data subjects typically within one month. If Stavanger Barnevaktbyrå decides not to comply with a request, the data subject will be notified of the reason.

4.4.6 In regard to supporting 3rd parties with their personal data accuracy, our DPO is responsible for making them aware of any change in circumstances that may affect the accuracy of their personal data storage or processing.

4.5 In form submission by the data subject, the personal data therein must be kept only as long as is necessary for secure processing.

4.5.1 Where applicable, personal data should be encrypted in order to protect the identity of the data subject in the event of a data breach.
4.5.2 Personal data that will be retained during a form submission process must be securely destroyed upon completion of the process.

4.5.3 Data storage that could exceed legit retention periods must be justified and approved in writing by the DPO.

4.6 When assessing appropriate technical measures for controlling or processing personal data operations, the DPO will consider the following:

- Password protection;
- Access rights for USB and other memory media;
- Company-wide cloud storage access rights;
- Virus checking software and firewalls;

- Encryption of devices that leave the organizations premises such as laptops;
- Security of local and wide area networks;
- Automatic locking of idle terminals.

5. Data subject

5.1 Stavanger Barnevaktbyrå recognizes the rights of the data subject as expressed in the GDPR and intends to fully support the data subjects in exercising these rights as they pertain to their personal data that is under the control of Stavanger Barnevaktbyrå or being processed by Stavanger Barnevaktbyrå.

6. Consent

6.1 Stavanger Barnevaktbyrå understands a data subject's 'consent' to mean that, upon the data subject being fully informed of the intended personal data processing operation, it has been freely given by a clear affirmative and mindful action and signifies agreement to the policies, terms and conditions that apply.

6.2 The data subject can withdraw his or her consent at any time by request to the DPO or, where applicable, use a service intended for that purpose.

6.3 Consent cannot be inferred from non-response to a communication, and where applicable, Stavanger Barnevaktbyrå will be able to demonstrate that consent was obtained for a personal data processing operation.

7. Personal data security

7.1 All personal data should be accessible only to those who are authorized to use it, and access may only be granted by the DPO to Stavanger Barnevaktbyrå staff, or 3rd party entities (under the constraint of a confidentiality agreement), with just cause. As such all personal data should be treated appropriately:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected; and/or
- stored on (removable) computer media which are encrypted

7.2 Stavanger Barnevaktbyrå's staff must take care to keep unauthorized personnel from viewing screens displaying personal data and follow other related security rules.

7.3 Physical materials displaying personal data may not be left where they can be accessed by unauthorized personnel and may not be removed from business premises without explicit authorization by the DPO.

8. Formal request for personal data

8.1 All formal requests, such as from an official law enforcement agency, to provide personal data must be supported by appropriate paperwork and all such disclosures must be specifically authorized by the DPO.

9. Retention and disposal

9.1 Stavanger Barnevaktbyrå shall not keep personal data beyond a period necessary for its original purpose(s).

9.2 Stavanger Barnevaktbyrå may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes provided that doing so will also safeguards the rights and freedoms of the data subjects.

9.3 The retention period for each information asset will be set out in Stavanger Barnevaktbyrå's Information Asset Register (IAR).

9.4 Personal data must be disposed of securely and in accordance GDPR.

10. Personal data transfer

10.1 All exports of personal data from within the European Economic Area (EEA) to third countries (non-EEA countries) are unlawful unless there is an appropriate level of protection for the rights of the data subjects. The transfer of personal data outside of the EEA is prohibited unless one or more of these specified safeguards, or exceptions, apply:

- An adequacy decision - based on the list of third countries that currently satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
- Privacy Shield - If Stavanger Barnevaktbyrå wants to transfer personal data from the EEA to an organization in the United States it should check that the organization is signed up with the Privacy Shield framework at the U.S. Department of Commerce.
- Contract clauses Stavanger Barnevaktbyrå may adopt that are approved by a supervisory authority.
- Exceptions:
  - the data subject has legally consented to the proposed transfer;
  - the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
  - the transfer is necessary for the conclusion or performance of a contract conducted in the interest of the data subject between the controller and other living natural person;
  - the transfer is necessary for valid reasons of public interest;
  - the transfer is necessary for the establishment, exercise or defense of legal claims; and/or
  - the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

11. Information Asset Register (IAR)

11.1 Stavanger Barnevaktbyrå has established the IAR to manage its personal data inventory as well as the life cycle of its information assets as determined by:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of responsible parties throughout the personal data's life-cycle;
- key systems and repositories;
- any data transfers; and

- all retention and disposal requirements.

11.2 By means of the IAR, all Stavanger Barnevaktbyrå management is aware of any risks associated with the processing of particular types of personal data and can act accordingly in order to best safeguard the freedoms and rights of data subjects.

11.2.1 The DPO assesses, and indicates within the IAR, the risk levels of particular information assets in order to establish guidelines for their management in compliance with the GDPR. Data protection impact assessments are performed in relation to the processing of personal data by Stavanger Barnevaktbyrå.

11.2.3 The DPO must approve of new technologies for any personal data storage or processing by performing DPIAs.

11.2.4 In the case that there are significant doubts concerning a particular information asset based on the results of a DPIA, either as to the potential for damage, breach, distress, or regarding quantity of data, the DPO will seek the counsel of a supervisory authority.

Effective: 18/08/2018