GDPR and Data Protection Policy

Developed	January 2018
Latest review	2025-06
Approved by / date	CN – Senior Management / 18 March 2024
Document owner	Director of Administration
Responsible Case Handler	Compliance Advisor
Next review due	Every 6 months

Introduction

Caritas Norway (hereafter CN) complies with the Norwegian Personal Data Act (LOV-2018-06-15-38), which aims to protect the individual against privacy violations through the processing of personal data.

CN needs to gather and use certain information about individuals. This includes data collected from employees, volunteers, donors, partners, beneficiaries, customers, suppliers, business contacts and other people with whom the organization has a relationship or may need to contact, whether in digital or physical form.

Scope

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and comply with the law.

Data protection law and principles

The General Data Protection Regulation (GDPR) was approved by the EU Parliament on 27 April 2016 (Regulation (EU) 2016/679). Enforcement date: 25 May 2018. The GDPR was incorporated into the EEA agreement and became applicable in Norway on 20 July 2018.

CN adheres to the following key principles of data protection:

a. **Lawfulness, Fairness, and Transparency:** We ensure that personal data is processed lawfully, fairly, and transparently.

b. **Purpose Limitation:** Personal data is collected for specified, explicit, and legitimate purposes, and it is not processed in a manner incompatible with those purposes.

c. **Data Minimization:** We only collect and process the data that is necessary for the purposes for which it was collected.

d. **Accuracy:** We take reasonable steps to ensure that personal data is accurate and kept up to date.

e. **Storage Limitation:** Personal data is retained for no longer than necessary for the purposes for which it is processed.

f. **Integrity and Confidentiality:** We implement appropriate technical and organizational measures to ensure the security, integrity, and confidentiality of personal data.

g. **Accountability:** CN is responsible for demonstrating compliance with data protection principles.

We consistently evaluate the following factors to guarantee the effective processing of data:

- **Understand Your Data**: Identify and document the personal data your organization processes, where it comes from, and with whom it is shared.
- **Consent and Legal Basis**: Ensure that you have a valid legal basis for processing personal data and obtain consent where necessary.
- **Data Subject Rights**: Be prepared to facilitate individuals in understanding their rights regarding their personal data.
- **Data Security Measures**: Implement appropriate technical and organizational measures to protect personal data from unauthorized access, disclosure, alteration, and destruction.
- **Data Breach Response Plan**: Have a clear plan in place to respond quickly and effectively to data breaches.
- **Regular Training and Awareness**: Provide training to your employees on data protection principles and their responsibilities for handling personal data.
- **Data Processing Agreements**: Establish contracts with third-party data processors to ensure they also comply with GDPR requirements when processing personal data on your behalf.
- **Joint Controller Agreements:** Establish contracts with third-party data controllers to regulate the party's respective responsibility for compliance with applicable personal data legislation when they are joint controllers.
- **Keep Records**: Maintain documentation of your data processing activities, including records of processing activities, privacy impact assessments, and data breach notifications.
- **Review and Update Policies**: Regularly review and update your data protection policies and procedures to reflect changes in legislation, technology, and business practices.
- **Seek Legal Advice**: Consider seeking legal advice to ensure compliance with GDPR and other data protection laws specific to your business operations and data processing activities.

People, risks and responsibilities

This policy applies to:

- The head office of CN
- All offices and Regional representations of CN
- All staff and volunteers of CN
- All contractors, suppliers and other people working on behalf of CN

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation. This can include:

• Names of individuals
• Postal addresses
• Email addresses
• Telephone numbers
• Any other information relating to individuals

Data protection risks

This policy ensures that CN:

• Complies with data protection regulations and follows good practice
• Protects the data privacy rights of staff, customers and partners
• Is open about how it stores and processes individuals' data
• Protects itself from the risks of a data breach

Responsibilities: General staff guidelines, storage and use

CN, represented by the Secretary-General, is the data controller for the organization's processing of personal data.

Everyone who works for or with CN has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

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

• The Director of Administration is responsible for:

- **Ensuring quality of systems:**
  - All systems, services and equipment used for storing data must meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
- **Authorization and Training:**
  - Ensuring that the employee is authorized to handle sensitive data based on their role.
  - Provide comprehensive training on data protection policies, GDPR requirements, and the organization's procedures for handling sensitive data.
- **Understanding Sensitive Data**:
  - Familiarize the employee with the types of sensitive data they may encounter in their role.
  - Emphasize the importance of treating all sensitive data with confidentiality.
- **Purpose of Data Processing:**

- Clearly communicate the specific purpose for which the sensitive data is being collected and processed.
- Confirm that the employee understands the legitimate reasons for processing the data.

- **Consent Management:**
  - If applicable, ensure that the employee is aware of any consent mechanisms in place for processing sensitive data.
  - Stress the importance of obtaining explicit consent when required.
- **Data Minimization:**
  - Instruct the employee to only collect and process the minimum amount of sensitive data necessary for the intended purpose.
- **Secure Handling:**
  - Emphasize the need to store and transmit sensitive data securely, using encrypted channels and password protection as necessary.
  - Implement physical security measures if dealing with hard copies of sensitive data.
- **Access Controls:**
  - Ensure that the employee has access only to the sensitive data required for their job responsibilities.
  - Implement role-based access controls to restrict unnecessary access.
- **Data Subject Rights:**
  - Educate the employee about data subject rights, including the right of individuals to access, rectify, and request the deletion of their data.
  - Provide guidance on how to handle requests from data subjects.
  - If joint controllership, ensure that the essence of the arrangement between the joint controllers is available to the data subject.
- **Data Breach Response:**
  - Clearly outline the steps to be taken in the event of a suspected or confirmed data breach.
  - In the case of a personal data breach, The Director of Administration shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
  - Stress the importance of reporting any security incidents promptly.
- **Confidentiality Agreement:**
  - Have the employee sign a confidentiality agreement or non-disclosure agreement, reinforcing their commitment to maintaining the confidentiality of sensitive data.
- **Third-Party Interaction:**
  - If applicable, provide guidance on how to interact with third-party vendors or partners when handling sensitive data.

- Ensure that third parties also adhere to data protection standards.

- **Regular Training Updates:**
  - Schedule regular training updates to keep employees informed about changes in data protection laws, policies, and procedures.
- **Record-Keeping:**
  - Maintain a record of processing activities under its responsibility, containing all the information listed in Article 30 nr. 1 GDPR.
  - Maintain a record of all categories of processing activities carried out on behalf of a controller, containing all the information listed in Article 30 nr. 2 GDPR.
  - Instruct the employee to maintain accurate records of their sensitive data processing activities.
  - Encourage documentation of any decisions made during the handling of sensitive data.
- **Data Disposal:**
  - Provide guidelines on secure and proper methods for disposing of sensitive data, whether in electronic or physical form.
- **Monitoring and Auditing:**
  - Establish mechanisms for monitoring and auditing employee activities involving sensitive data to ensure ongoing compliance.
- **Reporting and Communication:**
  - Encourage open communication between employees and the administration department or relevant authority.
  - Establish reporting channels for any concerns or questions related to sensitive data handling.
- **Legal Awareness:**
  - Emphasize the importance of legal compliance and encourage employees to seek guidance if unsure about the correct procedures for handling sensitive data.
- **Regular Review of Policies:**
  - Remind employees to regularly review data protection policies and procedures to stay informed about any updates or changes.

- Keeping the board updated about data protection responsibilities, risks and issues.

- That the organization responds to Data Subject Access Requests (DSARs) promptly, typically within one month of receiving the request.

Privacy policy

Individual privacy is important to CN. CN complies with the Personal Data Act, which aims to protect the individual against privacy violations through the processing of personal data. In CN's privacy policy, the organization informs about how CN collects and uses personal data.

The data subject has the right to know information about themself/itself that CN maintains in relation to donors, visitors and service users how the information is processed and by whom. Everyone also has the right to have information corrected or deleted.

It is up to each individual who visits CN's website whether they want to provide personal data, but this is necessary if, for example, they want to receive our newsletter, make a donation, sign up for a course or become a volunteer.

Read more about rights and CN's obligations at The Norwegian Data Protection Authority's website.

CN has the following privacy-related text on its website:

Websites, social media and newsletters

CN's website uses cookies to improve the user's experience of the website by learning more about how the information provided is used. This is done by placing a cookie in the user's browser. CN does not store information that can personally identify the user.

CN uses the analysis tool Google Analytics to look at user patterns on its website in order to provide visitors to www.caritas.no with the most relevant information about the organization. Through Facebook's advertising platform and associated cookies, data is collected about which pages visitors have viewed on its website. CN regularly conducts risk assessments related to the use of Google Analytics to ensure compliance with GDPR.

When users subscribe to CN's newsletter, CN stores the subscriber's email address. The email addresses are deleted if/whenever the subscriber chooses to unsubscribe from the newsletter.

Donors

CN does not store sensitive personal data in its register, except for what is legally required for reporting to the tax authorities.

Volunteers

As part of a background check on its volunteers, CN stores the volunteer's name, date of birth, address, telephone number and email address. Volunteers who work directly with children must also present an impeccable certificate of good conduct from the police, which CN registers as having been submitted, but does not store the certificate itself.

Course participants

When individuals register for a course via CN's website, CN asks for the registrant's phone number, name, email, postal address, level of education and gender. This is to maintain

statistics on those who participate in CN's courses and to be able to contact participants with important information related to the course.

Personal data and third parties

CN is liable for both its own compliance with the GDPR, and the compliance of the chosen processor. While the overall responsibility generally lies with the data controller, data processors also have responsibilities under the GDPR. The respective roles and relationships shall be governed by a written data processing agreement.

If CN transfers personal data to, or receives personal data from, a third party, CN ensures that there is a lawful reason for transferring that data under GDPR. Personal data is only shared with other companies or subcontractors who perform tasks on behalf of CN. CN's partners are also subject to the Personal Data Act and have a separate data processing agreement with CN regarding the processing of personal data and the security of this information.

Data subject rights

All persons registered by CN may request access to the information registered and how it is used. Such information will only be disclosed after a written and signed request to CN. In this way, CN ensures that information is not disclosed to unauthorized persons.

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, CN will disclose requested data. However, the administration department will ensure the request is legitimate, seeking assistance from the Director of Administration and from the company's legal advisers where necessary.