Norsk Data Protection Policy

Context and Overview

Key details

Policy prepared by:

Nicholas Andrews, Chief Technology Officer

Norsk European Wholesale Limited ("Norsk")

Approved by Board/Management: 01/04/2018

Purpose of Review: Compliance: General Data Protection Regulation

Next Policy Review Date: 01/10/2018

Policy Scope

This policy applies to:

- All Norsk sites
- All employees
- All contractors, suppliers, third parties and other people working on behalf of Norsk

Introduction

As a business Norsk needs to request and collate certain information about individuals. This may include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

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 General Data Protection Regulation (GDPR) that comes into effect on 25 May 2018.

"The purpose of the GDPR is to provide a set of standardised data protection laws across all the member countries. This should make it easier for EU citizens to understand how their data is being used, and also raise any complaints, even if they are not in the country where it is located."

Why this policy exists

This Data Protection Policy ensures Norsk:

- Complies with GDPR in all cases
- Protects the rights of employees, partners, customers and suppliers
- Is clear how it (Norsk) controls and processes the personal data of individuals
- Protects itself from the risk of a data breach

Data Protection Law

The EU's General Data Protection Regulation (GDPR) replaces the Data Protection Act 1998 and describes how organisations, including Norsk must collect handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or in any other form.

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall be:

“a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

Article 5(2) requires that:

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

Risks and Responsibilities

Data Protection Risks

This policy helps to protect Norsk from data security risks, including:

- Breach of confidentiality
- Reputational damage

Responsibilities

Everyone who works for or with Norsk has some responsibility for data collection, storage and ensuring it is processed on a lawful basis.

However, these people (below) have key areas of accountability which underpin the responsibilities of those above:

The Board of Directors is ultimately accountable for ensuring Norsk meets its obligations through:

- Keeping employees, customers and suppliers updated about data protection responsibilities, risks and issues
- Ensuring all data protection procedures meet the requirements of GDPR and are maintained in accordance with future legislation updates
- Arranging up to date data protection training and advice for all individuals covered in this policy
- Handling data protection questions from employees and anyone else covered by this policy
- Dealing with requests from individuals to see the data Norsk holds about them (also called subject access requests)
- Checking and approving any contracts or agreements with third parties that may act as a sub-processor

The Chief Technology Officer, is responsible for:

- Ensuring all systems, services and equipment used for storing data meets and in some cases exceed security standards
- Perform regular checks and system scans to ensure security hardware and software is functioning properly
- Seeking written confirmation of GDPR compliance from any third party-service the company is considering using to store or process data
- Approving any data protection statements attached to company (Norsk) communications such as emails and websites
- Addressing any data protection queries from customers, suppliers, or third parties

Employee Guidelines

- Norsk will provide data protection awareness training to all employees, contractors and confirm this upon request, in line with GDPR due diligence requests
- The only employees able to access data covered by this policy are those who need it for their work – a lawful/legal basis must exist and never beyond the initial purpose
- Personal data must not be shared informally. When access to confidential information is made, the employee (data subject) must request this through HR in writing
- Employees should keep all personal data secure and take adequate and sensible precautions and follow the guidelines provided by the company
- PC and Mobile Device passwords must be strong, not easily guessed, and never shared with anyone else
- Personal data must not be disclosed to unauthorised persons, either within the company or externally - always refer them to HR in the first instance
- Employees must request help from their line manager if they are unsure about any aspect of data protection

Hardware

All company equipment issued to individuals for them to perform their jobs is the property of Norsk. It is the individual responsibility to care for and safeguard this company property and equipment, keeping it in as close to new condition as possible. Our equipment: Desktop PC's, Laptops and mobile devices are encrypted to ensure the integrity of our work and communications using the Norsk network.

The use of personal devices in any form is not permitted to control, processes or transfer Company (Norsk) data.

Personal Data Storage

These rules describe how and where personal data should be safely stored. Questions about personal data storage can be directed to the Chief Technology Officer.

When personal data is stored on paper, it must be kept in a secure lockable place where unauthorised personnel cannot access, view or retrieve it.

The guidelines also apply to personal data that is stored electronically but has also been printed in paper form:

- When not required, the document/paper or files must be kept in a **locked drawer or filling cabinets**
- Employees are accountable for ensuring documents/paper and printouts are not placed/left where unauthorised personnel can view, i.e on a printer or on left face-up on a desk
- **Personal data printouts must be shredded** and disposed of securely when no longer required for their initial purpose

Servers containing personal data are sited in a secure server room with restricted access. When personal data is stored electronically, it must be protected from unauthorised access, accidental deletion and hacking attempts:

- Files must be **protected by strong passwords** which should be changed regularly. This includes files and folders
- Access to data storage on removable media, (USB, CD or DVD), without written request to IT via a Line Manager is denied in all cases
- Personal data must only be stored on designated drivers and servers
- Data is backed-up regularly, in line with the company's standard backup procedure.
- Data or Personal Data must never be saved directly to laptops or other mobile devices
- All servers and computing systems containing data are protected by a licenced industry approved security software and a firewall.

Use of personal data

Personal data is of no value to Norsk unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees must ensure the screens of their computer are always locked when left unattended
- Data is encrypted before being transferred electronically. The Chief Technology Officer will/can explain if an individual is unsure
- Employees must never save copies of personal data to their own computers
- Please speak to HR if you need make any changes to your personal data

Data Accuracy

The General Data Protection Regulation requires Norsk to ensure personal data in all its forms is kept accurate, relevant and up to date.

It is the responsible of all Data controllers to ensure personal data is kept accurate

- Data will be held in as few places as necessary. Employees are not permitted to make copies
- Norsk has procedures in place for data subjects to update the information we hold on them
- Data should be updated as inaccuracies are discovered

Data Subject Access Request

All data subjects have the right to:

- be informed of specific information about the processing of their data
- access their personal data and rectification of personal data if incomplete or inaccurate (free of charge)
- erase through deletion of personal data where no lawful basis for it to continue being processed exists
- be informed how the company (Norsk) is meeting its data protection obligations and GDPR compliance.

If an individual contacts Norsk requesting this information, this is called a Data Subject Access Request.

Access requests from individuals should be made by email or in writing addressed to the Data Controller responsible for the information they are requesting datasubjectaccessrequest@norsk-global.com

For verification purposes the Data Controller will always verify the identity of anyone making a subject access request before information is released.

The Data Controller will aim to provide relevant data within a month.

Disclosing Data to public authorities

Norsk will comply with GDPR guidance concerning the disclosure of personal data to public authorities:

- Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law.
- The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems.
- The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

Providing Information

Norsk's GDPR training ensures that all employees/clients are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

Norsk has a Privacy Policy, setting out how data relating to individuals is used by the company.

---- END ----