NAVIGATING GDPR

AN EXHAUSTIVE GUIDE FOR SMALL AND MEDIUM-SIZED BUSINESSES IN ESTONIA

FINTECH
LEGAL CENTER

The content provided in this publication is for informational purposes only. It is not intended to constitute professional advice of any kind. Readers are advised to seek professional advice tailored to their specific circumstances before making any decisions or taking any actions based on the information provided herein. **FinTech Legal Center** does not assume any responsibility or liability for any errors or omissions in the content, nor for any consequences arising from the use of the information contained within.

January 2024

Introduction

In the digital landscape of today, where data is the lifeblood of businesses, ensuring the protection and privacy of personal information is of paramount importance.
The General Data Protection Regulation (GDPR) serves as the cornerstone of data protection, imposing strict regulations on how businesses handle personal data.
For small and medium-sized businesses (SMBs) in Estonia, understanding and complying with GDPR is a legal obligation and a crucial step towards building trust with customers and avoiding substantial fines.
This comprehensive guide, tailored specifically for businesses operating in Estonia, will delve deeper into the critical aspects of GDPR, and its relevance to SMBs.

Understanding GDPR
A Deeper Dive

GDPR, enacted in 2018, represents a comprehensive set of regulations dictating how companies and organizations manage the personal data of employees, customers, and clients.
The core principles of GDPR, emphasizing responsible data processing and protection of individual rights, are echoed in the Estonian legal landscape.

Applicability to Estonian Small Businesses

The first question many SMBs in Estonia might ask is whether GDPR is applicable to them. The unequivocal answer is yes. Regardless of size, any business that handles personal data is obligated to comply with GDPR regulations. Personal data, as defined by GDPR, encompasses a broad range of information, including names, addresses, medical records, and customer reviews. Establishing a clear understanding of what constitutes personal data is the initial step towards compliance.

Size Matters: Tailoring Compliance to Business Size

While larger companies with 250 or more employees are mandated to comply with GDPR, smaller businesses are not exempt.
Estonian SMBs should pay close attention to the rules outlined by the Estonian Data Protection Inspectorate, especially if data processing is not a one-off occurrence, involves sensitive information, or uses particular category or criminal conviction data.

Navigating the Compliance Maze
A Step-by-Step Approach

Compliance with GDPR can seem like a daunting task, especially for SMBs. However, adopting a systematic approach can simplify the process and ensure that your business adheres to the necessary regulations.

Terminology Mastery: Speaking the Language of GDPR

Navigating the intricacies of the General Data Protection Regulation (GDPR) involves familiarising oneself with a specific set of terms that form the foundation of this comprehensive data protection framework.

Let's demystify some key concepts:

Data Subject: This refers to individuals whose personal data is collected, processed, or stored. In essence, it's the person to whom the data belongs.

Consent: Permission granted by the data subject for the processing of their personal data. Consent should be informed, specific, and given voluntarily.

Processing: The broad term encompassing any operation performed on personal data, including collection, recording, organization, storage, alteration, retrieval, and more.

Data Controller: The entity or individual determining the purposes and means of processing personal data. Businesses often act as data controllers in the context of customer data.

Data Processor: The entity or individual processing personal data on behalf of the data controller. This could be a third-party service handling specific data processing tasks.

Lawful Basis: The legal justification for processing personal data. GDPR outlines six lawful bases, including consent, contract, legal obligation, legitimate interests, vital interests, and public task.

Understanding these terms is vital for effective communication, ensuring compliance, and fostering a culture of data protection within your organisation. As we delve deeper into the intricacies of GDPR compliance, this knowledge will serve as a compass, guiding businesses through the maze of regulations and obligations.

Audit Your Personal Data: A Foundation for Compliance

Begin by creating a comprehensive list of the various types of personal data your company processes. This list should include categories such as customer addresses, client phone numbers, and customer reference numbers. The goal is not to document the actual personal information but to gain an understanding of the categories you handle regularly. This step serves as the foundation for GDPR compliance.

Consider the Purpose of Data Collection: "Why" and "How" Matter

After establishing the types of personal data, analyze the reasons and methods behind its collection. Ensuring that data collection is lawful and conducted with a legitimate reason is vital for compliance. Identify any data collected without proper consent, as GDPR places a strong emphasis on ensuring individuals are aware of and comfortable with how their data is used.

Understand Lawful Basis: The Pillars of GDPR Compliance

GDPR defines six lawful bases for processing personal data: consent, contract, legal obligation, legitimate interests, vital interests, and public task. Utilize the European Data Protection Board resources to determine the appropriate category for your data processing activities. Ensuring that your data processing aligns with one of these lawful bases is a crucial aspect of compliance.

Transparency in Data Usage: Building Trust through Communication

As a business owner, transparency is critical. Clearly communicate to individuals what data you are collecting, how it will be used, and why. Craft a comprehensive consent request that includes business details, purposes for data collection, and a withdrawal notice.

Building trust through transparent communication is not only a legal requirement but also a fundamental aspect of maintaining positive customer relationships.

Evaluate Data Entry Forms: Ensuring GDPR-Compliant Data Collection

Review your existing data entry forms to ensure GDPR compliance. Utilize consent-oriented options such as tick boxes, yes/no options, signatures, or opt-in buttons. The choices presented to individuals must be unambiguous, and maintaining an audit trail can be beneficial. Regularly evaluate and update your data entry forms to align with evolving GDPR regulations and best practices.

Respect Individual Rights: Upholding Privacy in Practice

Familiarise yourself with the eight individual rights granted under GDPR, including the right of access, right to object, right to be informed, right to rectification, and right to erasure:

- Right to be Informed: Clear and transparent communication on data processing.
- Right of Access: Individuals can request access to their personal data.
- Right to Rectification: Allows correction of inaccurate or incomplete data.
- Right to Erasure (or Right to be Forgotten): Individuals can request deletion of their data under certain conditions.
- Right to Restrict Processing: Limits how personal data is processed in certain situations.
- Right to Data Portability: Individuals can receive and transfer their data between services.
- Right to Object: Allows objection to processing of personal data for specific purposes.
- Rights Related to Automated Decision Making and Profiling: Protection against decisions made solely by automated processes.

Tailor your data processing operations to uphold these rights, ensuring individuals have control over their personal information. Establish processes within your business to promptly address requests related to these rights.

Align Business Operations with Individual Rights: Practical Considerations

Understand how individual rights relate to your specific business processes. For instance, if your business collects data for targeted marketing, consider how customers might exercise their rights, such as the right to object or request erasure. Integrating these considerations into your day-to-day operations not only ensures compliance but also demonstrates your commitment to respecting individual privacy.

GDPR and the Estonian System A Symbiotic Relationship

In the dynamic landscape of data protection, Estonia has seamlessly integrated the General Data Protection Regulation (GDPR) principles into its legal framework, fostering a symbiotic relationship that prioritizes individual privacy and business responsibility.

Estonia's commitment to upholding high data protection standards aligns with the core tenets of GDPR. The Estonian Data Protection Inspectorate's mission is to "protect people's privacy and help the state to be transparent".
Small and medium-sized businesses (SMBs) in Estonia find themselves navigating a regulatory landscape that not only adheres to local laws but also mirrors the principles outlined by GDPR.

As Estonia continues to champion innovation and digital transformation, the nation's legal system recognises the significance of harmonising with GDPR, ensuring a robust framework that safeguards personal data and engenders trust between businesses and their stakeholders. This alignment facilitates seamless compliance for enterprises operating within Estonia and underscores the nation's commitment to fostering a secure and transparent digital environment for its citizens.

fintechlegalcenter.eu

phone +372 602 8411
address Valge 13, 11415 Tallinn, Estonia
email welcome@fintechlegalcenter.eu