techstep

Techstep Essentials MDM

GDPR Pocket Guide

Date: 18/10/2023

Contents

1 What is GDPR 4
2 When can You process the personal data? 5
3 The new definition of personal data 6
4 Penalties and fines 6
5 Required technical standards 7
6 Security and corporate mobile devices 8
7 How does the Techstep Essentials MDM system help comply with GDPR requirements? 9

PUBLISHED BY:

Techstep Poland S.A.
Ul. Wajdeloty 12A
80-437 Gdańsk

1 What is GDPR

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect, it will replace the data protection directive (officially Directive 95/46/EC) of 1995. The regulation was adopted on 27 April 2016. It becomes enforceable from 25 May 2018 after a two-year transition period and, unlike a directive, it does not require national governments to pass any enabling legislation, and is thus directly binding and applicable.

2 When can You process the personal data?

Processing shall be lawful only if and to the extent that at least one of the following applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

3 The new definition of personal data

One of the major changes the GDPR introduces is the broadening of the definition of "personal data".
'Personal data' means **any information relating to an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

4 Penalties and fines

There will be two levels of fines based on the GDPR. The first is up to €10 million or 2% of the company's global annual turnover of the previous financial year, whichever is higher. The second is up to €20 million or 4% of the company's global annual turnover of the previous financial year, whichever is higher. The potential fines are substantial and a good reason for companies to ensure compliance with the Regulation.

5 Required technical standards

The GDPR does not specify minimum technical standards of data protection nor provides specific examples of best practices. Only indicates that:

- Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
- Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
- Controller must regularly test, measure and evaluate the effectiveness of technical and organizational measures to ensure processing safety

From 25th May 2018 each administrator has to take into account the nature, scope, context and purpose of the processing and the risk of violation of the rights or privacy of legal persons and will have to decide for themselves what kind of security, documentation and data processing procedures to implement.

As defined in Article 32 (1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1. the pseudonymisation and encryption of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6 Security and corporate mobile devices

Security policies should apply to all data processing hardware, including mobile devices, with due regard to the additional risks associated with mobility (lost device, theft, etc.).

Depending on the processing environment and objectives, appropriate policies may include, for example, the obligation to encrypt data stored on mobile devices, overlaying polarized displays on the monitor, which make it difficult to view the information in terms of whether the safety button device can be used to remove or encrypt the currently processed information.

Data administrators should also take into account the fact that more and more employees use their own smartphones, tablets and even laptops for their business purposes, which may be significantly different from those provided by the company's antivirus or anti-theft systems. control of the data controller. Hence, the common practice of many companies to allow the use of private equipment for business purposes has been the preparation of specific guidelines for employees.

7 How does the Techstep Essentials MDM system help comply with GDPR requirements?

7.1 Data backup and archiving

Backup and archiving are one of the basic legal regulations included in the GDPR. Entrepreneurs, regardless of whether they are state or private, will be obliged to carry out special processing registers in which they will have to confirm the use of backup and archiving policies.

7.2 Integration with Wi-Fi infrastructure

By integrating with network infrastructures (including Extreme Networks, Cisco, Checkpoint) Techstep Essentials MDM controls access to enterprise Wi-Fi networks, allowing restricted access to managed and policy-compliant devices. This solution provides an additional barrier protecting the data stored in the corporate network from potential data stealing.

For third-party applications, Techstep Essentials MDM offers the External Compliance Checker, which enables any IT solution to verify the security level of a mobile device that is seeking access to data. Only trusted devices that comply with applicable security policies, with encrypted data, will receive full access to the information they collect.

7.3 Force data encryption and access control

Techstep Essentials MDM integrated with Samsung KNOX and Android Work Profile enables complete separation between private and corporate data stored on the mobile device. Company does not have access to the files and information contained in the private part of the device.

In addition, Techstep Essentials MDM enforces trusted access to business services. Unauthorized access attempts may be blocked.

By using the Techstep Essentials MDM system, you can access information integrated with the Techstep Essentials MDM system itself (eg Company Mail, Calendar, etc.). This is because our secure data access (Techstep Essentials VPN) solution. When Techstep Essentials VPN is used, access to any corporate data is properly controlled.

7.4 Support due to data leakage

Another important change is the need to report without delay (within 72 hours after the breach) a data leakage incident to the supervisory authority.

This also applies to Techstep Essentials MDM. It collects logs that allow you to identify irregularities and take immediate action. Another example is to allow users to instantly report the loss or theft of a mobile device by Techstep Essentials MDM and erase the remote data from the device.

Techstep Essentials MDM also sends alerts when malware is , jailbreak or rootkit detected, or if the device is non-compliant with a security policy.

In addition, it protects potentially sensitive data on smartphones and tablets by automatically deleting data when a threat is detected (e.g., incorrect password entry, SIM card replacement or lack of connectivity to the MDM server for an extended period of time).