UNIKIE

General Data Protection Regulation

(GDPR)

Version: 1.0
Date: 07.05.2018

Author: Jari Mononen, CIO

EU template: Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now V2.0 20170525

Confidential

Introduction

This document highlights the steps Unikie has taken for the General Data Protection Regulation (GDPR) which will apply from 25 May 2018.

Many of the GDPR's main concepts and principles are much the same as those that are already in the current Data Protection Act (DPA), so most of the state of compliance steps will remain valid under the new GDPR act. The main changes are to make the company procedures visible and systematically documented, to deal with the GDPR's new transparency and individuals' rights provisions.

The GDPR places greater emphasis on the internal documentation to demonstrate the accountability. Compliance with all the areas are listed in this document and will require company to review the approach to governance and how to manage data protection as a corporate issue. One aspect of this is to review the contracts and other arrangements in place when sharing data with other organizations.

1. Awareness

Unikie takes GDPR seriously and ensures that decision makers and key people in our organization are aware that the law is changing towards the GDPR. Key persons and stakeholders are aware of the impact and are constantly identifying the areas that could cause compliance problems under the GDPR. Implementing the GDPR involves people from administration, information management, HR, recruiting, sales and accounting.

2. Information you hold

Unikie keeps track on all the personal data we hold, where it came from and who it is shared with. Unikie maintains records of the data processing activities and data accuracy.

The list of the Unikie data repositories is in Annex 1.

3. Communicating privacy information

Unikie has reviewed the current company privacy notice according to the GDPR. When collecting any personal information, Unikie explains how we intend to use that information. This is done through the privacy notice. In the privacy notice, we also explain the lawful basis for processing the data, the data retention periods and that individuals have a right to complain to the Information Commissioner's' Office (ICO), if they think there is a problem with the way we are handling their data. The ICO's Privacy notices code of practice reflects the new requirements of the GDPR.

4. Individuals' rights

Unikie's procedures ensure that they cover all the GDPR rights individuals have, including the steps how personal data is deleted or how the data is provided to individual.

The GDPR includes the following rights for individuals:

- the right to be informed, how stored data is used
- the right of access, to verify own personal data
- the right to rectification, to ask for data correction
- the right to erasure, for removing own data
- the right to restrict processing, or any utilization of given data

- the right to data portability, when applicable
- the right to object, when applicable
- the right not to be subject to automated decision-making including profiling, when applicable

Unikie stores personal data under GDPR only in recruiting candidate and company employee registers. So, most of the rights are natural and are related either to the data stored during the recruiting process or employee data during the employment.

5. Subject access requests

Unikie will comply in 30 days when subject access request (SAR) notice is received. SAR must be delivered in written format to Unikie and it will be processed without charge. Unikie is prepared to answer individual SAR requests related following details:

- what personal data it is being processed
- the purposes for which the personal data is being processed
- who, if anyone, the personal data is disclosed to
- the extent to which it is using the personal data for the purpose of making automated decisions relating to the data subject and, if so, what logic is being used for that purpose

The answer for the SAR is delivered in written format. It can be sent either using verified email address, fetch from Unikie Tampere office or sent using conventional mail.

6. Lawful basis for processing personal data

Unikie has the lawful basis for data processing activity according to the GDPR. Unikie has two main repositories containing personal data

Employee Register
Employee register contains the basic information of the people working for Unikie. The data collected is used for contacting the workforce, keeping track of the work hours done and bank details to be able to pay the salaries. The details of the data registered is specified in Annex 1.

Recruitment Register
Recruitment register contains the potential applicants for new job opportunities. The collected information including the personal details, contact information, talents and CVs with details of earlier job experiences are used for staffing and match making with open vacancies. The persons stored into the recruitment register have given the consent (chapter 7) for storing the information according to the Unikie Privacy Notice (chapter 3).

Unikie reviews the types of processing activities annually to identify the lawful basis for the data processing and to comply with the GDPR's 'accountability' requirements.

7. Consent

Unikie seeks, records and manages the person consent for storing the data into the Recruitment register. No data is stored into any register without given consent. In practice, when a person leaves an application and records the recruiting information, the person need to read and agree the given Unikie Privacy Notice. In case information is received directly and stored manually into the register, the consent is also asked from the person.

Consent to process any recruitment data is freely given, is specific for the recruitment purpose, is informed to the person and is unambiguous. The consent option in electronic forms is a positive opt-in – i.e., consent is not inferred from silence, pre-ticked boxes or user inactivity. Consent can also be verified according to the SAR (chapter 5).

Consent to record and process any personal data in Employee Register is received in written format when new work contract is signed.

8. Children

The GDPR sets the age when a child can give their own consent to this processing at 16. Unikie does not offer any online services to children and does not process any children's personal data under age at 16.

9. Data breaches

Unikie follows carefully the access rights, access statistics and anomalies on our data servers. We are prepared to detect, report and investigate a personal data breach. Organizations storing high risk information are required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. When Unikie does not process any data that would contain a risk to the rights and freedoms of individuals – such as discrimination, damage to reputation, major financial loss, loss of confidentiality or any other significant economic or social disadvantage – our data processed can be treated as low risk information.

10. Data Protection by Design and Data Protection Impact Assessments

Even when data we process can be treated as a low risk information, Unikie follows good design practices and adopts a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of GDPR. Only such information that is really required is collected and adequate security and privacy measures needed are implemented for decent data usage.

11. Data Protection Officers

Unikie does not need official Data Protection Officer (DPO) according to GDPR. However, Unikie's CIO has also additional responsibility for data protection compliance. CIO has the required knowledge, support and authority to carry out the role effectively.

12. International

Unikie operates in two member states inside EU – in Finland and Germany. The Unikie's lead data protection supervisory authority (LDPSA) is placed in Unikie's headquarters in Tampere, Finland. The Unikie's central administration and LDPSA will make the most significant decisions related to the GDPR.