AlfaPeople

Where to start with the GDPR

The General Data Protection Regulation

Introduction

A European privacy law is due to take effect on late May 2018 – more specifically May 25, 2018. The privacy law, the General Data Protection Regulation (GDPR for short), which is all about the protection and enabling of the privacy rights of individuals, will set a new bar globally regarding issues such as security, privacy rights and compliance. How you manage and protect personal data while at the same time respecting every individual choice will be established and governed by GDPR – and the requirements will be there no matter where you send your data, process it or store it.

This whitepaper will help you prepare for the GDPR, providing an overview of the new European privacy law. You'll get all the answers you need in order to get started with the process – including how AlfaPeople can help your compliance with the GDPR where your Microsoft Dynamics platform is concerned.

Understanding the GDPR

What is the GDPR exactly?

GDPR – The General Data Protection Regulation – is a new European privacy law. More specifically, it is a privacy regulation reaching across the European Union, providing individuals with more control than previously over their personal data and ensuring transparency about the use of data. Additionally the GDPR requires security and controls to protect data.

Why do I need to know this – does the GDPR apply to my organization at all?

It may be tempting to believe that the GDPR only applies to very specific organizations. However, looking closely it becomes apparent that it applies more broadly than might be apparent at first glance. In fact, the GDPR imposes new rules on companies, government agencies, non-profits, and other organizations offering goods and services to people in the European Union (EU), or companies, government agencies, non-profits, and other organizations collecting and analyzing data tied to EU residents. And the law applies no matter where the organizations are located in the world. Where privacy laws in other jurisdictions may not apply to all types and sizes of organizations, the GDPR doesn't take size or type of industry into consideration; it applies to everyone. The GDPR may not continually be restricted to the EU – as the European Union often is considered a role model on privacy issues internationally, the GDPR concepts are in time expected to turn up in other parts of the world.

This GDPR - when does it take effect?

As mentioned above, the GDPR officially takes effect on May 25, 2018, even though it already became law in the EU back in April 2016. The reason for it not taking effect officially until 2018 is that it entails significant changes, which some organizations will need to align with, making a two-year transition period a necessity. The GDPR is replacing the existing Data Protection Directive (Directive 95/46/EC), which has been in force since 1995.

GDRP key concepts

The GDPR may seem complex, but the key concepts can be broken down into six principles.

1. Requiring transparency on how the handling and use of personal data takes place.
2. Limiting personal data processing to specified, legitimate purposes.
3. Limiting personal data collection and storage to intended purposes.
4. Making it possible for individuals to correct or request deletion of their personal data.
5. Limiting the storage of personally identifiable data for only as long as necessary for its intended purpose.
6. Ensuring that personal data is protected using appropriate security practices.

Examples of GDPR requirements related to these principles

• If an organization is processing personal data, under the GDPR, **individuals have a right to know** that as well as to be informed of (and understand) **the purposes of that processing**. If individuals want to have their data deleted or corrected, or if individuals don't want their data processed any longer, want to object to direct marketing, want to revoke consent for certain uses of their data, etc., it is their right.

And because of the right to data portability, individuals also have the right to move their data elsewhere – and to receive assistance in doing so.

• Under the GDPR, **organizations must secure personal data** in accordance with its sensitivity. If a data breach occurs, the relevant authorities must generally be notified within 72 hours by the data processors. If the breach is likely to result in a high risk to the rights and freedoms of individuals, affected individuals must be notified by the organizations without undue delay.

• **Processing of personal data must be conducted on a legal basis**. Consent for the processing of personal data must be "freely given, specific, informed, and unambiguous." Where children are concerned, the GDPR includes unique consent requirements.

• In order to predict the privacy impacts of projects and employ mitigations as needed, **organizations must conduct data impact assessments.** Meaning that records of processing activities, consents to process data and compliance with the GDPR must be maintained.

• GDPR compliance is an ongoing process, and non-compliance with the GDPR can result in significant fines. **Organizations are encouraged to embrace a culture of privacy** to protect the interests of individuals in their personal data in order to ensure GDPR compliance. Both Microsoft and AlfaPeople are committed to help you meet the GDPR requirements and to further support the privacy rights of individuals. Please visit Microsoft.com/GDPR for a more detailed overview of the GDPR and a better understanding of terms like pseudonymization, processing, controllers, processors, data subjects, and personal data.

Get help to your GDPR journey with Microsoft

It is a business-wide challenge to be GDPR compliant. A challenge that will require time, tools, processes, and expertise, and it will most likely also require significant changes in your practices of privacy and data management. Operating in a well-architected cloud services model will make the journey towards GDPR compliance smoother – as will an effective data governance program. Microsoft and AlfaPeople are ready to help you successfully comply with the GDPR in an efficient and professional manner.

Cloud service you can trust is Microsoft in a nutshell. Microsoft takes a principled approach to privacy, security, compliance, and transparency with strong commitments, so you can rest assured that you can trust the digital technology you need and rely on. Microsoft holds the most extensive compliance portfolio in the industry, and the organization was the first to adopt key standards such as the ISO/IEC 27018 cloud privacy standard. Moreover, Microsoft is an experienced leader in privacy, security, compliance, and transparency – something both customers and partners benefit from.

GDPR - getting started

Most of your IT landscape is likely to be subject to the requirements of the GDPR. The reason why, is that the systems you use to create, store, analyze, and manage data can be spread across a wide array of IT environments—personal devices, on-premises servers, cloud services, even the Internet of Things.

Looking at the GDPR requirements holistically and within the context of all your regulatory and legal privacy obligations will best serve your efforts to meet the requirements and be compliant. The GDPR isn't the only data protection around, and thus many of the security controls to prevent, detect, and respond to vulnerabilities and data breaches required by the GDPR are similar to the controls expected by e.g. the ISO 27018 cloud privacy standard.

It is very time-consuming to track controls required by individual standards or regulations on a case-by-case basis. Best practice will be to identify an overall set of controls and capabilities to meet these requirements, the same way that taking a platform view (e.g. Windows, Microsoft SQL Server, SharePoint, Exchange, Office 365, Azure, and Dynamics 365) can provide a clearer path to compliance with not only the GDPR, but also other requirements important and relevant to you. Often, individual technologies and solutions are assessed against a comprehensive regulation such as the GDPR, but that is much too time-consuming.

Facilitate your journey to GDPR compliance with the following four KEY STEPS:

Discover

Identify your personal data and where it resides.

Protect

Establish security controls to prevent, detect, and respond to vulnerabilities and data breaches

Manage

Govern how your personal data is used and accessed.

Report

Execute on data requests, report data breaches, and keep required documentation (Business Intelligence) and Cortana Intelligence Suite features.

12 questions you need to address now

By reading and preparing these 12 questions from the Danish Data Protection agency you can stay ahead of GDPR by taking action today*.

1. Does your organization know about the GDPR?

It is important to ensure that decision-makers and key figures in your organization is aware that the personal data protection act will be replaced by the GDPR in 2018. You should also check how your organization will be affected by the GDPR and identify the areas you need to pay special attention to and work specifically on.

2. What kind of personal data do you process?

You should screen and document which personal data you process, where the data comes from, and who you share the data with. Moreover, you may need to examine your organization in order to find out, which personal data is processed in which part of the organization.

3. What kind of information do you give the registered?

You should examine the information you give to the registered and consider which changes of that information may be necessary under the GDPR.

4. How do you meet the rights of the registered?

You should scrutinize your procedures in order to ensure that you can meet all the rights of the registered under the GDPR.

The most important rights of the registered under the GDPR is as follows:

- The right to get information regarding processing of your own personal data (duty to disclose all material facts)
- The right to gain insight into your personal data.
- The right to get incorrect personal data rectified
- The right to get your personal data deleted
- The right to take exception to the use of personal data for direct marketing purposes
- The right to take exception to automatic individual decisions, including profiling/marketing
- The right to move your personal data (data portability)

It is a good idea to go through your routines already by now and consider how you will manage a request for e.g. the deletion from a registered person. Can your system help you find and eventually delete the data? Who in your organization can make a decision about deletion?

* https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/12_spoergsmaal_-_GDPR.pdf

5. On which grounds do you process personal data?

You should examine which categories of personal data you process and on which grounds you do it. You should at the same time document your conclusions.

6. How do you obtain consent?

You should investigate how you obtain, store and document consent and if you should make any changes.
7. Du you process children's personal data?
You should already be considering how you will check a person's age in the future, and how you will obtain consent from the custody holder, when you in certain situations process children's personal data.

7. Du you process children's personal data?

You should already be considering how you will check a person's age in the future, and how you will obtain consent from the custody holder, when you in certain situations process children's personal data.

8. What should you do about breaches of the personal data security?

You should make sure that you are in control of the required procedures in order to detect, report and investigate breaches of the personal data security.
9. Are your procession associated with specific risks?
You should consider whether or not your processing of personal data is associated with specific risks of the fundamental rights of the registered, and, if so, you should prepare an impact analysis regarding data protection in agreement with the GDPR.

9. Are your procession associated with specific risks?

You should consider whether or not your processing of personal data is associated with specific risks of the fundamental rights of the registered, and, if so, you should prepare an impact analysis regarding data protection in agreement with the GDPR.

10. Do your IT systems include data protection?

You can, with advantage, already now take the requirements of the GDPR into consideration when you start using a new IT system or make changes to an existing system. It will make it easier for you to comply with the GDPR and enhance security.

11. Who is responsible for data protection matters in your organization?

You should consider where you will place the responsibility of data protection matters in your organization. In certain situations the GDPR will encompass requirements on formally appointing a DPO – a data protection advisor.

12. Do you conduct business in more countries than one?

If your organization conducts business in more than one EU country, you should find out which supervisory authority is in charge of inspection your processing of personal data.

How AlfaPeople can help you getting GDPR compliant

AlfaPeople is a Gold Microsoft Partner and Cloud CRM Partner of the Year in Denmark. We will strive to help our customers getting GDPR compliant. We are used to working with large, international projects within CRM and ERP, more precisely Microsoft Dynamics 365 solutions. These solutions often involve a great amount of personal information, security demands and Change Management. Thus, our experience makes us able to understand how the GDPR requirements need to be addressed.

AlfaPeople can help you getting ready for the GDPR with a 3-step approach involving assessment and analysis of processes supported by the Microsoft Dynamics 365 platform. With a thorough analysis, we can provide customers with actionable insights into areas and processes affected by GDPR, and subsequently help to prioritize, plan and implement measures which reduces the workload of achieving compliance for those processes and solutions.

To get more information about how **AlfaPeople** can help you and your company getting ready for the **GDPR** – don't hesitate to contact us.

Phone: +45 70 20 27 40
Email: info.dk@alfapeople.com

Global Offices

AlfaPeople - Headquarters
Støberigade 14, 4. sal
2450 **København** SV
Denmark
Phone: +45 70 20 27 40
Email: info.dk@alfapeople.com

AlfaPeople United Kingdom
Phoenix House
18 King William Street,
London, EC4N 7BP
Phone: +44 330 223 0635
Email: info.uk@alfapeople.com

AlfaPeople US
Chrysler Building
405 Lexington Avenue,
26th Floor, **NY** 10174
Phone: +1 (855) 732-6484
Email: info.us@alfapeople.com

AlfaPeople Germany
Elsbach Haus, Goebenstraße 3-7
32052 **Herford**
Phone: +49 5221 28440-0
Fax +49 5221 28440-44
Email: info.de@alfapeople.com

AlfaPeople Switzerland
Hohenbühlstrasse 2
8152 **Glattbrugg**
Phone: +41 43 355 30 60
Fax: +41 43 355 30 61
Email: info.ch@alfapeople.com

AlfaPeople Colombia
Ave Cra 9 # 123-86
Edificio Uraki – Ofi 401, **Bogotá**
Phone: +571 6054222
Fax: + 571 2082198
Email: info.co@alfapeople.com

AlfaPeople Chile
Avda. Nueva de Lyon 072
Oficina 801, Piso 8
Providencia, **Santiago**
Phone: +56 (2) 2 751 90 00
Mobile: +56 9 75296062
Email: info.cl@alfapeople.com

AlfaPeople Brazil - Barueri
Al. Tocantins, 125 – Conj. 250,
Alphaville Industrial
06455-931
Barueri-SP
Phone: +55 (11) 4082-3232
Email: info.br@alfapeople.com

AlfaPeople Brazil - Porto Alegre
Rua Mostardeiro, 366
5° andar
90430-001
Porto Alegre
Phone: +55 (51) 2117-1865
Email: info.br@alfapeople.com

AlfaPeople Costa Rica
Calle 36. Av 4 y 6.
Edificio Don Bosco. Tercer Piso
San Jose
Phone: +506 2233 7000
Fax +506 2233 3238
Email: info.cr@alfapeople.com

AlfaPeople Guatemala
5ta Avenida 4-55 Zona 14
Edificio Europlaza Torre 1, 2do Nivel,
Oficina 208/209
Phone: +502 2386 9981
Fax: +502 2386 8800
Email: info.gt@alfapeople.com

AlfaPeople Mexico
Baja California # 245 Piso 8
Colonia Hipódromo.
Condesa C.P. 06170
México, D.F.
Phone: +55 5265 6030 Ext.878
Email: info.mx@alfapeople.com

AlfaPeople China
Four Seasons Square, Building 2
No. 503 NingGuo Road,
Shanghai
200090
Phone: +966 2 6929450
Email: kle@alfapeople.com

AlfaPeople United Arab Emirates
Sidra Tower (1801)
Sheikh Zayed Road
PO Box 9588, **Dubai**
Phone: +971 4 5585066
Fax: +97144405988
Email: info.me@alfapeople.com

AlfaPeople Saudi Arabia
King Road Tower (1106)
King Abdulaziz Road – **Jeddah**
PO Box 11787, Jeddah 21463
Phone: +966 2 6929450
Fax: +966 2 6068744
Email: info.me@alfapeople.com

Microsoft Partner
Microsoft
Gold Cloud Platform
Gold Cloud Productivity
Gold Enterprise Resourse Planning
Gold Customer Relationship Management
Gold Cloud Customer Relationship Management
2017/2018 INNER CIRCLE for Microsoft Dynamics