GEDERD knows how to comply with the GDPR easily

Needs and Solutions Matrix

squalio

Introduction

This GDPR Needs and Solution Matrix sets out the key requirements that the General Data Protection Regulation will introduce into EU Privacy law on 25 May 2018. The matrix highlights the most important actions which businesses should take to prepare for compliance.

The GDPR will apply to companies processing personal data in the context of an EU establishment, companies offering goods or services to EU residents and companies that monitor the behavior of EU residents. The changes brought in by the GDPR are wide-reaching and will be affected by the changes, from marketing to security and, of course, legal and compliance.

Matrix

GDPR ISSUES	GDPR REFERENCE	EXPLANING DETAILS	SAMPLES OF DAY TO DAY CASES WHEN GDPR ISSUES APPEAR	ACTIONS TO BE MADE	SUGGESTED IT SOLUTIONS WITHIN OFFICE365 E3
Lawfulness of data use	article 6, 7, 8	Data of individuals can be used: 1. if the individual consented; 2. if required according to law. Individual - data owner has rights to withdraw his consent.	1. One may collect data of individuals either by writing them down, receiving them by email or collecting passport copies of individuals because it is more convenient to later make or control records related to particular individual. 2. One may collect copies of ID or passport thinking that this guarantees that one has verified identity of the individuals, but such approach is not required/permitted by law.	1. Detect what is basis for collection and use of data. 2. Obtain consent of data owner. 3. Delete data according to request of data owner.	1. SharePoint Online - foundational document management.
Classification of data	article 9, 10, 11	One should recognize what categories of data he has. High level groups: public, confidential. Possible sub-classification: commercial secret, internal use information, HR related data, financial data, IT data etc. Special category: sensitive data.	1. Although one may want to know if employee is pregnant, belongs to trade union or political party, there are very limited cases when laws and regulations permit to collect this type of information. 2. Practice shows that people do not understand which information is confidential, when and where they risk by using information. Therefore it is important to indicate which type of information shall be especially protected.	1. Key words are created to sort/ select the information - name, surname, number (e.g. personal identity number), address, street, house number, city. 2. Detect if data are in means of record where it is difficult to access them, sort by key words (e.g. pdf passport copies, offsite servers).	1. Office 365 eDiscovery - finds your data . 2. Labelling by Office 365 - according to key words the data can be automatically or manually labeled per category (e.g. automated label - confidential, manual sub-label - internal data).

GDPR ISSUES	GDPR REFERENCE	EXPLANING DETAILS	SAMPLES OF DAY TO DAY CASES WHEN GDPR ISSUES APPEAR	ACTIONS TO BE MADE	SUGGESTED IT SOLUTIONS WITHIN OFFICE365 E3
Access rights	article 12, 13, 14, 15, 16, 17, 18, 20, 21, 22 article 24, 27, 28	Every access to any data shall be granted only in case access to the data is really required for the particular individual to perform his/her duties.	1. If all files and systems are available to all employees in the company there is no protection neither to sensitive information of the company, nor personal data of individuals. Lack of access restrictions includes high risk of information leakage. 2. Controlled system of access rights will help company to detect who accessed information and leaked, and to claim recovery of damages from specific employee. This helps also to prove basis for dismissal.	1. Access to data on personal level (my data). 2. Access to data on company level (data of others). 3. User Ids. 4. Creating and protecting passwords. 5. Segregation of access rights based on information and employee id.	1. Creation of user IDs, user groups - groups have access to certain folders/files. 2. Creation of sub-access to certain individuals – Office 365 Groups, Office 365 active directory (AD) ensures mandatory creation of certain users. 3. Passwords – Office 365 sets criteria for permitted passwords.
Resource used	article 24, 26, 28	Knowing the resource used helps to determine the security measures to be applied. Resources could be: 1. Equipment/ Software used. 2. Email. 3. Internet access. 4. Mobile and portable devices. 5. Installing software. 6. Network shared disks. 7. Personal owned devices.	1. One may have forgotten about servers or data storage places held. Irrespective of where held all such information is subject to protection. 2. Using private emails for business purposes does not provide sufficient security for data flow and user access control. 3. Using unsecured/ not sufficiently secure cloud or using devices without passwords makes easier for third persons (e.g. robbers) to access information on such devices.	1. Decrease diversity of resources used. 2. Use safe resources providing long-lasting storage, processing and solutions.	1. Migrate all data to cloud - Office 365 cloud storage. 2. Protection by rule that only safe tools can be used - Office 365 MDM. 3. Content Search and Audit logs applicable across all Office 365.

GDPR ISSUES	GDPR REFERENCE	EXPLANING DETAILS	SAMPLES OF DAY TO DAY CASES WHEN GDPR ISSUES APPEAR	ACTIONS TO BE MADE	SUGGESTED IT SOLUTIONS WITHIN OFFICE365 E3
Retention of records	article 30	Data shall be retained according to internal procedures of the data holder and according to requirements of the applicable laws.	1. Each piece of information has certain storage/ retention period either established by law or applied by company. Not following such information storage rules may result for the company in facing fines imposed by law or other type of liability. 2. Storing information accordingly also safeguards that company can provide documentary evidences on actions or omissions if so required, e.g. in a dispute/court case. It is important because one can sue others as long as the claim rights have not expired (sometimes for 10 years).	1. Ensure technical possibility to retain data for the required period. 2. Sort data per category, per term of storage. 3. Follow when data storage term ends and data shall be deleted/ destroyed.	1. Retention tags based on Labels and Sensitive information types. 2. Automatic deletion or hold of the information according to the set Retention Policy.
Supervision	article 24, 26, 28, 30	All actions performed with data shall be recorded, stored and monitored.	1. Controlled system of access rights will help company to detect who accessed information and leaked, and to claim recovery of damages from specific employee. This helps also to prove basis for dismissal. 2. Internal audits may help to find weak spots in the company security systems, which systems are more often accessed and who did that.	1. Monitoring – IT personnel monitors the system in general, follows the actions performed with data. 2. Record extraction available to select data stored in the system regarding certain individual. 3. Trail of actions, records stored. 4. Internal/ External audit performed from time to time.	1. Record extraction - Office 365 eDiscovery. 2. Monitoring, trail of actions, records - Office 365 Version history 3. Audits of data and services - Office 365 Auditing.

GDPR ISSUES	GDPR REFERENCE	EXPLANING DETAILS	SAMPLES OF DAY TO DAY CASES WHEN GDPR ISSUES APPEAR	ACTIONS TO BE MADE	SUGGESTED IT SOLUTIONS WITHIN OFFICE365 E3
Security	article 32, 33, 34	Access to data and data processing shall be safe.	1. If no security systems in place employees do not use information with due care, they also tend to send to others data which are to be protected. If one would leak data of other individuals the company shall have obligation to report such leakage to state authorities supervising data protection, as well as inform individuals on the fact that their data have been leaked. This results in liability established by law both for the company - holder of the data, as well as employee who leaked the data. 2. Back up of data ensures that company complies with requirements of law related to storage of documents.	1. Reporting security incidents (internal/ external) to IT admin, to compliance officer, to state authorities, to data owner. 2. Ensure recovery of security – not only technical solutions shall be implemented but also manually the data holder should monitor and ensure security of the data. 3. Ensure back up of data.	1. Alerts on data illegal access/ use - Office 365 Alerts, alert soft and detailed reports per period are available. 2. Recovery of security – Microsoft ongoing support for security for Office 365 users. 3. Back up – O365 entirely itself, manufacturer ensures several servers, full data restore is available.

squalio

GEDERD knows how to comply with the GDPR easily

www.gederd.com

squalio