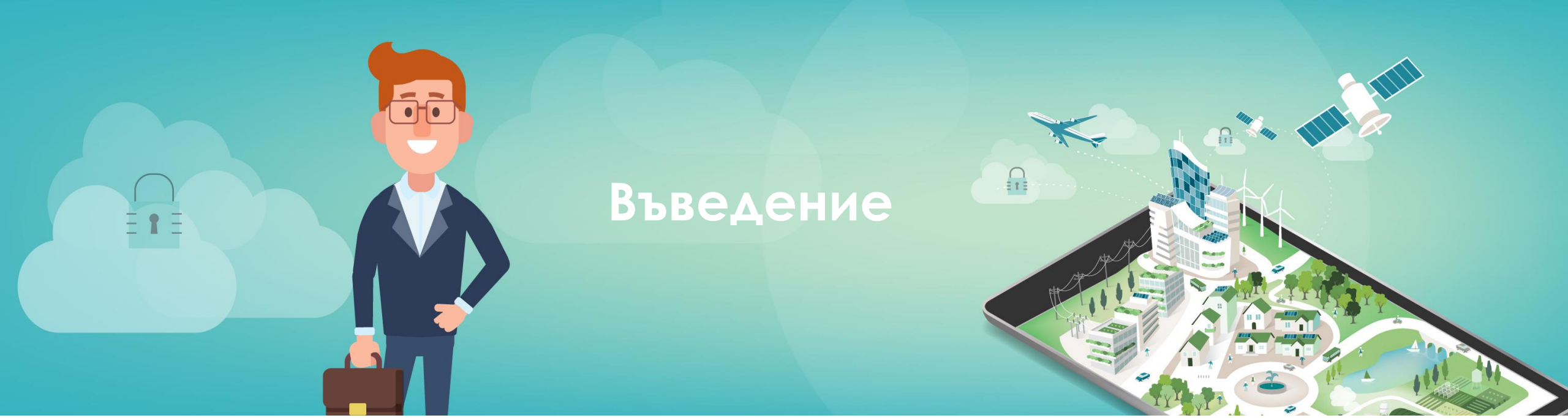
Гого знае как лесно да отговори на изискванията на ОРЗД

Матрица за проблеми и решения относно ОРЗД

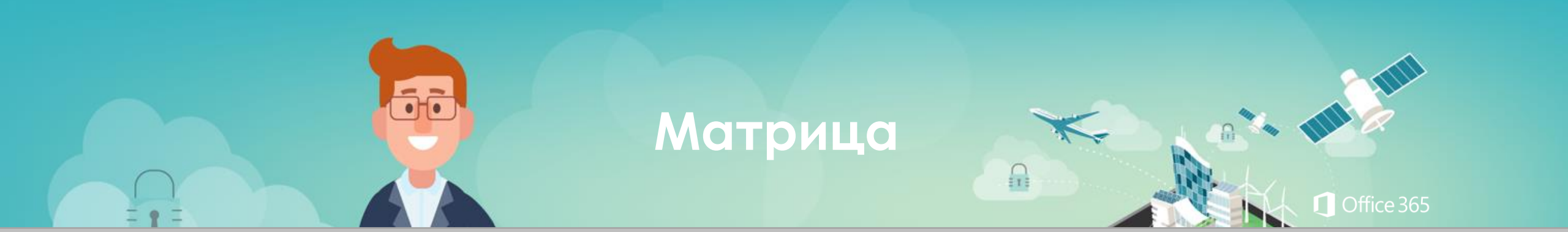
squalio



Въведение

Тази матрица за проблеми и решения относно ОРЗД определя основните изисквания, които Общият регламент за защита на данни ще въведе в Закона за защитата на лични данни на ЕС на 25 май 2018 г. Матрицата очертава най-важните действия, които предприятията трябва да предприемат, за да се подготвят да отговорят на условията.

ОРЗД ще се прилага за дружества, които обработват лични данни в контекста на Европейско предприятие, фирми, предлагащи стоки или услуги на жители на ЕС и компании, които следят поведението на жителите на ЕС. Промените, въведени от ОРЗД, са широкообхватни и ще засегнат области от маркетинга до сигурността, разбира се, от правна гледна точка и в съответствието с изискванията.



Матрица

ОСНОВНИ ПРОБЛЕМИ ПО ОТНОШЕНИЕ НА ОРЗД	ПРЕПРАТКИ В ОРЗД	ПОДРОБНО ОБЯСНЕНИЕ	ПРИМЕРИ ОТ ЕЖЕДНЕВИЕТО КОГАТО ВЪЗНИКНАТ ВЪПРОСИ ЗА ОРЗД	ПРЕДПРИЕМАНЕ НА ДЕЙСТВИЯ	ИТ ПРЕДЛОЖЕНИЯ И РЕШЕНИЯ В ОФИС365 Е3
Законност на използването на данни	Членове 6, 7, 8	Данните на физическите лица могат да бъдат използвани: 1. ако лицето е дало съгласие; 2. ако се изисква, съгласно закона. Физическото лице - собственик на данните има право да оттегли своето съгласие.	1. Възможно е да събирате данни за физически лица, като ги записвате на хартия, получавате ги по електронна поща или събирате паспортни копия, защото е по-удобно по-късно да се съхранява или контролира архив, свързан с конкретното лице. 2. Възможно е да събирате копия на лични карти или паспорти, считайки, че това гарантира, че сте проверили самоличността на лицата, но този подход не се изисква/разрешава от закона.	1. Открийте каква е целта на събирането и използването на данни. 2. Вземете съгласието на титуляра на данните. 3. Изтрийте данните, по искане на титуляра на данните.	1. SharePoint Online - фундаментално управление на документи.
Класификация на данни	Членове 9, 10, 11	Всеки трябва да знае какви категории данни притежава. Групи на високо ниво: публични, поверителни. Възможни под-категории: търговска тайна, информация за вътрешна употреба, данни, свързани с човешките ресурси, финансови данни, ИТ данни и др. Специална категория: чувствителни данни.	1. Въпреки че може да искате да знаете дали една служителка е бременна, принадлежи към синдикат или политическа партия, има много ограничени случаи, когато законите и подзаконовите актове позволяват събирането на този вид информация. 2. Практиката показва, че хората не разбират коя информация е поверителна, кога и къде рискуват, когато използват информация. Ето защо е важно да се посочи кой тип информация трябва да бъде специално защитена.	1. Създават се ключови думи за сортиране/избор на информация - име, фамилия, номер (например личен идентификационен номер), адрес, улица, номер на апартамент, град. 2. Открийте дали данните са в записи, които ги правят трудно достъпни, сортирайте по ключови думи (например копия на паспорти, външни сървъри).	1. Офис 365 eDiscovery - открива Вашите данни. 2. Категоризиране от Офис 365 - според ключови думи данните могат автоматично или ръчно да се категоризират (например автоматизиран етикет - поверително, ръчен под-етикет - вътрешни данни).

ОСНОВНИ ПРОБЛЕМИ ПО ОТНОШЕНИЕ НА ОРЗД	ПРЕПРАТКИ В ОРЗД	ПОДРОБНО ОБЯСНЕНИЕ	ПРИМЕРИ ОТ ЕЖЕДНЕВИЕТО КОГАТО ВЪЗНИКНАТ ВЪПРОСИ ЗА ОРЗД	ПРЕДПРИЕМАНЕ НА ДЕЙСТВИЯ	ИТ ПРЕДЛОЖЕНИЯ И РЕШЕНИЯ В ОФИС365 Е3
Достъп до права	Членове 12, 13, 14, 15, 16, 17, 18, 20, 21, 22 Членове 24, 27 и 28	Всеки достъп до каквито и да било данни се предоставя само в случай, че действително се изисква достъп до данните, за да може дадено лице да изпълнява своите задължения.	1. Ако всички файлове и системи са достъпни за всички служители на компанията, няма защита нито на чувствителната информация на компанията, нито на личните данни на физическите лица. Липсата на ограничения по отношение на достъпа включва висок риск от изтичане на информация. 2. Контролирана система за права на достъпа ще подпомогне компанията да разбере кой е получил достъп до информация и как тя е изтекла, както и да иска възстановяване на вредите от конкретния служител. Това помага и за доказване на основанието за освобождаване от длъжност.	1. Достъп до данни на лично ниво (моите данни). 2. Достъп до данни на фирмено ниво (данни на други лица). 3. Идентификационен номер на потребителя. 4. Създаване и защита на пароли. 5. Разпределение на права за достъп въз основа на тип информация и идентификационен номер на служителя.	1. Създаване на потребителски идентификационни номера, потребителски групи - групите имат достъп до определени папки/файлове. 2. Създаване на под-достъп на определени лица - Групи в Офис 365, Активна Директория в Офис 365 (Active Directory (AD)), които осигуряват задължително създаване на определени потребители. 3. Пароли - Офис 365 определя критерии за разрешени пароли.

ОСНОВНИ ПРОБЛЕМИ ПО ОТНОШЕНИЕ НА ОРЗД	ПРЕПРАТКИ В ОРЗД	ПОДРОБНО ОБЯСНЕНИЕ	ПРИМЕРИ ОТ ЕЖЕДНЕВИЕТО КОГАТО ВЪЗНИКНАТ ВЪПРОСИ ЗА ОРЗД	ПРЕДПРИЕМАНЕ НА ДЕЙСТВИЯ	ИТ ПРЕДЛОЖЕНИЯ И РЕШЕНИЯ В ОФИС365 Е3
Използвани ресурси	Членове 24, 26 и 28	Познаването на използвания ресурс помага да се определят мерките за сигурност, които да се прилагат. Ресурсите могат да бъдат: 1. Използвано оборудване/софтуер. 2. Електронна поща. 3. Интернет достъп. 4. Мобилни и преносими устройства. 5. Инсталиране на софтуер. 6. Споделени мрежови дискове. 7. Лични устройства.	1. Може да сте забравили къде на сървърите или на други места съхраненявате данни. Независимо къде се съхранява, тази информация подлежи на защита. 2. Използването на лични и-мейл адреси за бизнес цели не осигуряват достатъчна сигурност за потока от данни и контрола на достъпа на потребителите. 3. Използването на незащитен или недостатъчно сигурен облак или използването на устройства без пароли улеснява достъпа на трети лица (например крадци) до информацията върху такива устройства.	1. Намалете разнообразието на използваните ресурси. 2. Използвайте безопасни ресурси, осигуряващи дългосрочно съхранение, обработка и решения.	1. Прехвърлете всички данни в облак - облака за съхранение на Офис 365. 2. Защита с правило, че могат да се използват само безопасни инструменти - Office 365 MDM. 3. Търсачка за Съдържание и Одит логове, приложими в целия Офис 365.

ОСНОВНИ ПРОБЛЕМИ ПО ОТНОШЕНИЕ НА ОРЗД	ПРЕПРАТКИ В ОРЗД	ПОДРОБНО ОБЯСНЕНИЕ	ПРИМЕРИ ОТ ЕЖЕДНЕВИЕТО КОГАТО ВЪЗНИКНАТ ВЪПРОСИ ЗА ОРЗД	ПРЕДПРИЕМАНЕ НА ДЕЙСТВИЯ	ИТ ПРЕДЛОЖЕНИЯ И РЕШЕНИЯ В ОФИС365 Е3
Запазване на записи	Членове 24, 26, 28, 30	Всички действия, извършени с данни, ще се записват, съхраняват и наблюдават.	1. Контролираната система за права на достъп ще помогне на компанията да разбере кой е получил достъп до информация и от къде е изтекла тя, както и да иска възстановяване на вредите от конкретния служител. Това помага и за доказване на основанието за освобождаване от длъжност. 2. Вътрешните одити могат да помогнат да се открият слабите места в системите за сигурност на компанията, кои системи са по-често достъпни и кой е направил това.	1. Мониторинг - ИТ персонал, който да следи системата като цяло, да проследява действията, извършвани с данни. 2. Възможност за извличане на записи, за да се изберат данни, съхранявани в системата по отношение на определени лица. 3. Проследяване на действия, съхраняване на записи. 4. Периодично извършване на вътрешен/ външен одит.	1. Извличане на записи - Офис 365 eDiscovery. 2. Мониторинг, проследяване на действия, записи - Офис 365 Version history 3. Одити на данни и услуги - Офис 365 Auditing.
Сигурност	Член 32, 33, 34	Достъпът до данните и обработката на данните са защитени.	1. Ако няма предвидена система за сигурност, служителите не използват информацията с дължимата грижа и също така са склонни да изпращат данни, които би трябвало да са защитени, на други лица. Ако някой разкрие данни за други лица, компанията е задължена да докладва за изтичането на информация на държавните органи, които контролират защитата на данните, както и да информира лицата за факта, че техните данни са изтекли. Това води до отговорност, предвидена в закона, както за дружеството - притежател на данните, така и за служителя, който е причина за изтичането им. 2. Резервно копие (Back up) на данните гарантира, че дружеството отговаря на законовите изисквания, свързани със съхранението на документи.	1. Докладване на инциденти във връзка със защитата (вътрешна/външна) на ИТ администратор, на служител по съответствието, на държавните органи, на собственика на данните. 2. Гарантиране на възстановяването на защитата – ще бъдат внедрени не само технически решения, но също така притежателят на данните ръчно следва да наблюдава и гарантира сигурността на данните. 3. Осигурете резервно копие на данните.	1. Сигнали за нелегален достъп/използване на данни - Офис 365 Alerts дава възможност за подробни периодични доклади. 2. Възстановяване на сигурността – Постоянна поддръжка на Майкрософт за сигурност за потребителите на Офис 365. 3. Резервни копия (Back up) - О365 изцяло самостоятелно, като производителят осигурява няколко сървъра с пълно възстановяване на данните.

Гого знае как лесно да отговори на изискванията на ОРЗД

www.gogogdpr.bg

squalio