ОБЩ РЕГЛАМЕНТ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
(EU General Data Protection Regulation - GDPR)

ОПЕРАТИВНО РЪКОВОДСТВО

ЗА МАЛКИТЕ И СРЕДНИ ПРЕДПРИЯТИЯ ,

ЗА ВНЕДРЯВАНЕ НА ИЗИСКВАНИЯТА, В СЪОТВЕТСТВИЕ С GDPR И ЗАКОНА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ (проект)

1.Задължения на МСП (администратор и/или обработващ лични данни) по сигурността

Цел

Организацията трябва да определи, дали изпълнява своите задължения, съгласно изискванията на GDPR.

1.1Общи въпроси

• Организацията изпълнява ли своите задължения, при обработката налични данни ?

Контрол

Член от GDPR , определящ изисквания, свързани с МСП	**Контроли (сигнатура по ISO 27002:2013) свързани със съответните членове на GDPR**	**Допълнителни контроли (сигнатура по ISO 27018:2014) свързани със съответните членове на GDPR (при използване на публични „облачни“ услуги за обработка на лични данни)”.=6**
Чл.24 (1) (отговорности на администратора) **Администратора е отговорен за спазването на правилата, както те са описани в GDPR. Освен това, администратора, трябва да може покаже / докаже, че спазването се извършва на практика, чрез документи, контроли и др. , както е приложимо.**	A.5.1.1 (политика за информационна сигурност) **Контрол** Трябва да бъде определен набор от политики за сигурност на информацията, одобрен от ръководството, разпространен и разгласен на всички служители и съответните външни страни. A.5.1.2 (преглед на политиките за информационна сигурност) **Контрол** Политиките за сигурност на информацията трябва да бъдат подлагани на преглед през планирани интервали или при настъпване на значителни промени,	**Препоръки** Политиките за информационна сигурност трябва да бъдат доразвити, чрез ясно деклариране, свързано с поддръжката и поемането на ангажименти за постигане на съответствие с приложимите изисквания за защита на личната информация, произтичащи от закон и/или договор между оператора на публичен „облак“, обработващ лични данни и съответния администратор (потребител науслугите по обработка на личните данни в „облака“) Съответния договор трябва да определи отговорностите на оператора на публичния „облак“ (обработващ данни) , неговите подизпълнители и потребителите на“облачни“ услуги (администратор), като се отчита типа на тези услуги – IaaS (инфраструктура, като услуга), PaaS (платформа, като услуга) или SaaS

	за да се гарантира постоянно тяхната актуалност, адекватност и ефикасност. A.18.2.2 (съответствие с политиките и стандартите за информационна сигурност) **Контрол** Ръководителите трябва редовно да преглеждат доколко обработването на информация и процедурите в тяхната област на отговорност съответстват на подходящите политики за сигурност, стандарти и всякакви други изисквания за сигурност.	(софтуер, като услуга). Например, определянето на отговорностите за контроли по сигурността на приложно ниво, може да бъде различно, в зависимост дали се предоставят Saas, PaaS или IaaS услуги, на базата на които, администратора може да изгради собствени приложения,свързанис личните данни.
Чл.24 (2) (отговорности на администратора) Администратора трябва да вземе решение за политиките за защита на личните данни, вкл. , за съответните процедури, инструкции и контроли по сигурността.	A.5.1.1 (политика за информационна сигурност) **Контрол** Трябва да бъде определен набор от политики за сигурност на информацията, одобрен от ръководството, разпространен и разгласен на всички служители и съответните външни страни. A.5.1.2 (преглед на политиките за информационна сигурност) **Контрол** Политиките за сигурност на информацията трябва да бъдат подлагани на преглед през планирани интервали или при настъпване на значителни промени, за да се гарантира постоянно тяхната актуалност, адекватност и ефикасност.	**Препоръки** Политиките за информационна сигурност трябва да бъдат доразвити, чрез ясно деклариране, свързано с поддръжката и поемането на ангажименти за постигане на съответствие с приложимите изисквания за защита на личната информация, произтичащи от закон и/или договор между оператора на публичен „облак“, обработващ лични данни и съответния администратор (потребител науслугите по обработка на личните данни в „облака“) Съответния договор трябва да определи отговорностите на оператора на публичния „облак“ (обработващ данни) , неговите подизпълнители и потребителите на“облачни“ услуги (администратор), като се отчита типа на тези услуги – IaaS (инфраструктура, като услуга), PaaS (платформа, като услуга) или SaaS (софтуер, като услуга). Например, определянето на отговорностите за контроли по сигурността на приложно ниво, може да бъде различно, в зависимост дали се предоставят Saas, PaaS или IaaS услуги, на базата на които, администратора може да изгради собствени приложения,свързанис личните данни.
Чл.25 (1) (защита на данните по проект / при проектиране и по подразбиране) и (2) (защита на данните по проект / при проектиране и по подразбиране) **Администратора трябва за реши, какви подходящи технически и организационни мерки, и**	A.5.1.1 (политика за информационна сигурност) **Контрол** Трябва да бъде определен набор от политики за сигурност на информацията, одобрен от ръководството, разпространен и разгласен на всички служители и съответните външни страни. A.6.1.5 (информационната сигурност	**Препоръки** Политиките за информационна сигурност трябва да бъдат доразвити, чрез ясно деклариране, свързано с поддръжката и поемането на ангажименти за постигане на съответствие с приложимите изисквания за защита на личната информация, произтичащи от закон и/или договор между оператора на публичен „облак“, обработващ лични данни и съответния администратор (потребител науслугите по

защити (напр., псевдонимизация) ще внедри, отчитайки целите, обработките, рисковете и възможните последици за субектите на данни. **По подразбиране, трябва да е осигурено, че се обработва само информацията, свързана с изпълнението на целите .(на обработките)**	при управлениетонапроекти) **Контрол** Независимо от вида на проекта трябва да бъде отчетена сигурността на информацията при управление на проекти. A.14.1.1 (изисквания за сигурност към информационните системи) **Контрол** Изискванията, имащи отношение към сигурността на информацията, трябва дабъдат включени в изискванията за нови информационни системи или подобряване на съществуващи информационни системи. A.14.2.5 (принципи да сигурност при системния инжинеринг) **Контрол** Инженерни принципи за сигурни системи трябва да бъдат създадени, документирани, поддържани и приложени при всеки опит за реализиране на информационна система.	обработка на личните данни в „облака“) Съответния договор трябва да определи отговорностите на оператора на публичния „облак“ (обработващ данни) , неговите подизпълнители и потребителите на“облачни“ услуги (администратор), като се отчита типа на тези услуги – IaaS (инфраструктура, като услуга), PaaS (платформа, като услуга) или SaaS (софтуер, като услуга). Например, определянето на отговорностите за контроли по сигурността на приложно ниво, може да бъде различно, в зависимост дали се предоставят Saas, PaaS или IaaS услуги, на базата на които, администратора може да изгради собствени приложения,свързанис личните данни.
Преамбюл 78 (защита на данните по проект / при проектиране в случай на процедури за търгове) **Администратора трябва да реши, дали е необходимо да има срециални изсквания по сигурността към доставчика, извършващ ИТ проектирането, с цел да осигури, че съответните технически и/или организационни мерки / контроли са избрани и приложени.**	A.15.1.1 (политика за информационна сигурност при взаимоотношения с доставчици) **Контрол** С доставчика трябва да бъдат договорени и документирани изисквания за сигурност на информацията, които намаляват рисковете, свързани с достъпа на доставчика до активите на организацията. A.15.1.2 (разглеждане на сигур-ността в рамките на споразумения с доставчици) **Контрол** Всички приложими изисквания към сигурността на информацията трябва да бъдат въведени и съгласувани с всеки доставчик, който може да има достъп, да обработва, да съхранява, да разпространява или да предоставя ИТ инфраструктурни компоненти за информацията на организацията.	Няма допълнителен контрол

	A.13.2.2 (споразумения за обмен на информация) **Контрол** При прехвърляне на информация за дейността между организацията и външни страни трябва да бъдат сключвани споразумения.	
Чл.28 (1) (администратор) **Администратора ще използва само обработваща данните организация, която може да внедри подходящи технически и организационни мерки за сигурност. На база договор с администратора, обработващия данни ще осигури съответните гаранции, че ще внедри подходящи технически и организационни мерки за сигурност на личните данни.**	A.15.1.1 (политика за информационна сигурност при взаимоотношения с доставчици) **Контрол** С доставчика трябва да бъдат договорени и документирани изисквания за сигурност на информацията, които намаляват рисковете, свързани с достъпа на доставчика до активите на организацията. A.15.1.2 (разглеждане на сигурността в рамките на споразумения с доставчици) **Контрол** Всички приложими изисквания към сигурността на информацията трябва да бъдат въведени и съгласувани с всеки доставчик, който може да има достъп, да обработва, да съхранява, да разпространява или да предоставя ИТ инфраструктурни компоненти за информацията на организацията. A.13.2.1 (Политики и процедури за обмен на информация) **Контрол** Трябва да съществуват официални политики, процедури и механизми за контрол, за да се защити обмена на информация чрез използване на всички средства за комуникация. A.13.2.2 (споразумения за обмен на информация) **Контрол** При прехвърляне на информация за	**Препоръки** Когато за трансфера на информация се използват физически носители, трябва да има изградена система, чрез която да се регистрират входящите и изходящи физически носители, съдържащи лични данни, вкл., и типа на физическите носители; оторизираните податели и получатели; дата и време; брой на физическите носители. Когато е възможно, може да се приложат допълнителни мерки за сигурност (напр., криптиране на данните), с цел да се осигури, че данните могат да бъдат достъпни само в крайната (планираната) точка за получаване, а не по пътя на трансфера.

	дейността между организацията и външни страни трябва да бъдат сключвани споразумения.	
Чл.28 (2) (обработващ данни) **Администратра трябва да осигури, че обработващия данни няма да използва подизпълнители без предварително съгласуване и одобряване.**	A.15.1.1 (политика за информационна сигурност при взаимоотношения с доставчици) **Контрол** С доставчика трябва да бъдат договорени и документирани изисквания за сигурност на информацията, които намаляват рисковете, свързани с достъпа на доставчика до активите на организацията. A.15.1.2 (разглеждане на сигурността в рамките на споразумения с доставчици) **Контрол** Всички приложими изисквания към сигурността на информацията трябва да бъдат въведени и съгласувани с всеки доставчик, който може да има достъп, да обработва, да съхранява, да разпространява или да предоставя ИТ инфраструктурни компоненти за информацията на организацията. A.13.2.1 (Политики и процедури за обмен на информация) **Контрол** Трябва да съществуват официални политики, процедури и механизми за контрол, за да се защити обмена на информация чрез използване на всички средства за комуникация. A.13.2.2 (споразумения за обмен на информация) **Контрол** При прехвърляне на информация за дейността между организацията и външни страни трябва да бъдат сключвани споразумения.	**Препоръки** Когато за трансфера на информация се използват физически носиттели, трябва да има изградена система, чрез която да се регистрират входящите и изходящи физически носители, съдържащи лични данни, вкл., и типа на физическите носители; оторизираните податели и получатели; дата и време; брой на физическите носители. Когато е възможно, може да се приложат допълнителни мерки за сигурност (напр., криптиране на данните), с цел да се осигури, че данните могат да бъдат достъпни само в крайната (планираната) точка за получаване, а не по пътя на трансфера.
Чл. 28 (3) (обработващ данни) **В договора между администратора и обработващия данни, трябва да бъде осигурено, че обработващия данни:** **-ще обработва личните данни, на база**	A.9.2.2 (Осигуряване на достъп на потребители) **Контрол** Трябва да бъде реализиран официален процес за предоставяне на достъп на потребителите, който да предостави или отнеме правата за достъп на всички видове потребители до всички системи и услуги.	A10.13 Достъп до данни, намиращи се във вече използвано пространство за съхраняване на данни **Контрол** Обработващия данни, който е и оператор на публичен облак, трябва да осигури, че когато дадено пространство за съхранение на данни е присвоено на даден потребител на услуги, то този потребител няма да има

инструкциите на администратора; **-ще разрешава достъп до лични данни само на опълномощен за това персонал;** **-ще предоставя информация за провеждане на анализ на риска и съответно за внедряване на съответните мерки за сигурност;** **-ще подпомага администратора при дейностите му, свързани с осигуряването на правата на субектите на данни;** **-ще осигурява необходимите документи за провеждане на разследвания на пробиви в сигурността, а също и за нуждите за провеждане на оценката на въздействието;** **-ще има способности да изтрива или да връща всички лични данни на администратора;** **-ще поддържа в налично и актуално състояние цялата документация, свързана със съответствието с този член (Чл.28) на GDPR;** **Обработващия лични данни ще информира администратора, ако получените инструкции за обработката на лични данни са незаконосъобразни.**	A.9.4.1 (Ограничаване на достъпа до информация) **Контрол** Трябва да бъде ограничен достъпът до информация и функциите на приложните системи в съответствие с политиката за контрол на достъпа. A.12.1.1 (Документирани процедури за работа) **Контрол** Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях. A.13.2.2 (споразумения за обмен на информация) **Контрол** При прехвърляне на информация за дейността между организацията и външни страни трябва да бъдат сключвани споразумения. A.15.1.1 (политика за информационна сигурност при взаимоотношения с доставчици) **Контрол** С доставчика трябва да бъдат договорени и документирани изисквания за сигурност на информацията, които намаляват рисковете, свързани с достъпа на доставчика до активите на организацията. A.15.1.2 (разглеждане на сигурността в рамките на споразумения с доставчици) **Контрол** Всички приложими изисквания към сигурността на информацията трябва да бъдат въведени и съгласувани с всеки доставчик, който може да има достъп, да обработва, да съхранява, да разпространява или да предоставя ИТ инфраструктурни компоненти за информацията на организацията. A.16.1.3 (Докладване за слабости в сигурността на информацията) **Контрол**	възможност за виждане на данните, които вече са били съхранявани в това пространство. A.11 (съответствие с тайната на информацията за самоличността) A.11.1 Географско разположение на информация за самоличността **Контрол** Организациите поддържащи (оператор) публичен „облак“ и изпълняващи обработка на лични данни (обработващ лични данни) на администратори, трябва да определят и документират страните, в които личните данни могат да бъдат съхранявани. A.11.2 Планирани места за получаване на информация за самоличността **Контрол** Информацията за самоличността, предавана чрез мрежите за обмен на данни, трябва да бъде контролирана, с цел да се осигури, че е пристигнала на планираното място за получаване.

	Трябва да се изисква от служителите и доставчиците, използващи информационните системи и услуги на организацията, да отбелязват и докладват всяка наблюдавана или предполагаема слабост в сигурността в системите или услугите.	
Чл. 30(1) (записи за операциите по обработката на данни) **Администратора трябва да документира:** **- име и информация за контакт с него;** **- целта на обработките;** **- категориите субекти на данни, лични данни и възможни получатели;** **- трансферите налични данни;** **- периода за обработка на лични данни;** **- мерките за сигурност на личните данни;** **- взаимодействията с надзорните органи.**	A.12.1.1 (Документирани процедури за работа) **Контрол** Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях.	A.11 (съответствие с тайната на информацията за самоличността) A.11.1 Географско разположение на информация за самоличността **Контрол** Организациите поддържащи (оператор) публичен „облак“ и изпълняващи обработка на лични данни (обработващ лични данни) на администратори, трябва да определят и документират страните, в които личните данни могат да бъдат съхранявани. A.11.2 Планирани места за получаване на информация за самоличността **Контрол** Информацията за самоличността, предавана чрез мрежите за обмен на данни, трябва да бъде контролирана, с цел да се осигури, че е пристигнала на планираното място за получаване.
Чл. 30(2) (записи за операциите по обработката на данни) **Администратора трябва да документира:** **- име и информация за контакт с него;** **- категориите обработки,които се извършват от негово име;** **- трансферите налични данни;** **- мерките за сигурност на личните данни;** **- взаимодействията с надзорните органи.**	A.12.1.1 (Документирани процедури за работа) **Контрол** Процедурите за работа трябва да бъдат документирани и достъпни за всички потребители, които се нуждаят от тях.	A.11 (съответствие с тайната на информацията за самоличността) A.11.1 Географско разположение на информация за самоличността **Контрол** Организациите поддържащи (оператор) публичен „облак“ и изпълняващи обработка на лични данни (обработващ лични данни) на администратори, трябва да определят и документират страните, в които личните данни могат да бъдат съхранявани. A.11.2 Планирани места за получаване на информация за самоличността **Контрол** Информацията за самоличността, предавана чрез мрежите за обмен на данни, трябва да бъде контролирана, с цел да се осигури, че е пристигнала на планираното място за получаване.
Чл.32 (1, 2) (сигурност на обработките) **Администратора и обработващия данни провеждат анализ на риска, с основна насока**	A.5.1.1 (политики за информационна сигурност) **Контрол** Трябва да бъде определен набор от политики за сигурност на информацията, одобрен от	**Препоръки** Политиките за информационна сигурност трябва да бъдат доразвити, чрез ясно деклариране, свързано с поддръжката и поемането на ангажименти за постигане на съответствие с приложимите изисквания за

към личните данни. На базата на резултатите от проведения анализ на риска, организацията ще избере и внедри съответните мерки за сигурност – контролни и защитни механизми (технически и организационни)	ръководството, разпространен и разгласен на всички служители и съответните външни страни. A.6.1.5 (сигурност на информацията при управление на проекти) **Контрол** Независимо от вида на проекта трябва да бъде отчетена сигурността на информацията при управление на проекти. A.14.1.1 (анализ и спецификация на изискванията за сигурност на информацията) **Контрол** Изискванията, имащи отношение към сигурността на информацията, трябва да бъдат включени в изискванията за нови информационни системи или подобряване на съществуващи информационни системи. A.14.2.5 (принципи за сигурносх при системния инжинеринг) **Контрол** Инженерни принципи за сигурни системи трябва да бъдат създадени, документирани, поддържани и приложени при всеки опит за реализиране на информационна система.	защита на личната информация, произтичащи от закон и/или договор между оператора на публичен „облак“, обработващ лични данни и съответния администратор (потребител науслугите по обработка на личните данни в „облака“) Съответния договор трябва да определи отговорностите на оператора на публичния „облак“ (обработващ данни) , неговите подизпълнители и потребителите на“облачни“ услуги (администратор), като се отчита типа на тези услуги – IaaS (инфраструктура, като услуга), PaaS (платформа, като услуга) или SaaS (софтуер, като услуга). Например, определянето на отговорностите за контроли по сигурността на приложно ниво, може да бъде различно, в зависимост дали се предоставят Saas, PaaS или IaaS услуги, на базата на които, администратора може да изгради собствени приложения,свързанис личните данни.
Чл.32 (1) (а) (сигурност на обработките) **Администратора и обработващия данни ще преценят дали да включат в мерките за сигурност криптиране и псевдонимизация на личните данни**	A.10.1.1 (политика за използване на криптографски механизми за контрол) **Контрол** Трябва да бъде разработена и провеждана политика за използването на криптографски механизми за контрол с цел защита на информацията. A.9.4.1 (Ограничаване на достъпа до информация) **Контрол** Трябва да бъде ограничен достъпът до информация и функциите на приложните системи в съответствие с политиката за контрол на достъпа.	**Препоръки** Оператора на публичен облак, изпълняващ и обработкана лични данни (обработващ данни) трябва да предоставя до своите потребители, информация, свързана с обстоятелствата определящи използването на криптография и информация за своите способности, които могат да подпомогнат съответния потребител да приложи своя криптографска защита. **Забележка:** В няко случаи мож да има законови изисквания за криптиране на някои видоме лични данни – напр., здравна информация, номер на паспорт, номер на шофьорска книжка и др. A10.13 Достъп до данни, намиращи се във вече използвано пространство за съхраняване на данни **Контрол** Обработващия данни, който е и оператор на публичен облак, трябва да осигури, че

		когато дадено пространство за съхранение на данни е присвоено на даден потребител на услуги, то този потребител няма да има възможност да вижда данните, които вече са били съхранявани в това пространство.
Чл.32 (1) (в) (сигурност на обработките) **Администратора и обработващия данни трябва да осигурят непрекъснато високо ниво на информационна сигурност и устойчивост чрез прилагане на подходящи мерки за сигурност, на база проведена оценка на риска.**	A.5.1.1 (политики за информационна сигурност) **Контрол** Трябва да бъде определен набор от политики за сигурност на информацията, одобрен от ръководството, разпространен и разгласен на всички служители и съответните външни страни. A.14.1.1 (анализ и спецификация на изискванията за сигурност на информацията) **Контрол** Изискванията, имащи отношение към сигурността на информацията, трябва да бъдат включени в изискванията за нови информационни системи или подобряване на съществуващи информационни системи. A.14.2.5 (принципи за сигурносх при системния инжинеринг) **Контрол** Инженерни принципи за сигурни системи трябва да бъдат създадени, документирани, поддържани и приложени при всеки опит за реализиране на информационна система.	**Препоръки** Политиките за информационна сигурност трябва да бъдат доразвити, чрез ясно деклариране, свързано с поддръжката и поемането на ангажименти за постигане на съответствие с приложимите изисквания за защита на личната информация, произтичащи от закон и/или договор между оператора на публичен „облак“, обработващ лични данни и съответния администратор (потребител науслугите по обработка на личните данни в „облака“) Съответния договор трябва да определи отговорностите на оператора на публичния „облак“ (обработващ данни) , неговите подизпълнители и потребителите на“облачни“ услуги (администратор), като се отчита типа на тези услуги – IaaS (инфраструктура, като услуга), PaaS (платформа, като услуга) или SaaS (софтуер, като услуга). Например, определянето на отговорностите за контроли по сигурността на приложно ниво, може да бъде различно, в зависимост дали се предоставят Saas, PaaS или IaaS услуги, на базата на които, администратора може да изгради собствени приложения, свързанис личните данни.
Чл.32 (1) (с) (сигурност на обработките) **Администратора и обработващия данни ще осигурят възстановяване на личните данни в разумно (приемливо) време**	A.12.3.1 (резервиране на информацията) **Контрол** Трябва да бъдат направени и редовно изпитвани резервни копия на информация, софтуер и образи на системите в съответствие с договорената политика за резервиране. A.17.1.1 (планиране на непрекъснатост на сигурността на информацията) **Контрол** Организацията трябва да определи своите изисквания за сигурност на информацията и за непрекъснатост	**Препоръки** Когато обработващия данни е и оператор на публичен облак, и изпълнява услуги за резервиране (backup) и възстановяване, той трябва да предоставя информация, свързана със способностите си за тези услуги. Обработващия данни, когато е и оператор на публичен облак трябва да има политика за резервиране на личните данни, а също и за сигурно изтриване.

	на управлението на сигурността на информацията в неблагоприятни случаи, например по време на криза или бедствие. A.17.1.2 (iОсъществяване на непрекъснатост на сигурността на информацията) **Контрол** Организацията трябва да създаде, документира, осъществи и поддържа процеси, процедури и механизми за контрол, за да осигури необходимото ниво на непрекъснатост за сигурността на информацията по време на неблагоприятни случаи.	
Чл.32 (1) (d) (сигурност на обработките) **Администратора и обработващия данни трябва да осигурят, че мерките за сигурност ще бъдат тествани и оценявани.**	A.14.2.8 (Изпитване на сигурността на системата) **Контрол** По време на разработването трябва да бъдат изпитани функционалните възможности по отношение на сигурността. A.14.2.9 (Приемни изпитвания на системата) **Контрол** За нови информационни системи, подобрения и нови версии трябва да бъдат създадени програми за приемно изпитване и свързани с тях критерии. A.12.7.1 (Механизми за контрол при одит на информаци- онни системи) **Контрол** Изискванията за одит и действията, включващи проверки на работещи системи, трябва да бъдат внимателно планирани и съгласувани, за да се минимизират нарушенията на процесите на дейността. A.15.2.1 (Наблюдение и преглед на услуги, предоставяни от доставчици) **Контрол** Организациите трябва редовно да наблюдават, преглеждат и одитират предоставянето на услуги от доставчиците.	**Препоръки** Обработващия лични данни, който е и оператор на публичен облак, трябва да предостави на своите потребители на услуги независими доказателства за приложените мерки за информационна сигурност (напр., резултати от одити от сертификационна организация) и за практическото прилагане на политиките, и процедурите за сигурност на личната информация, обработвана в облака. Незамвисимия одит по информационната сигурност и защитата на личните данни в публичния облак е много приемлив метод за потребителите на облачни услуги, защото получават необходимата и достатъчна увереност, че техните интереси (свързани със личните данни) са защитени.

	A.18.2 (Независим преглед на сигурността на информацията) **Контрол** През планирани интервали или при настъпили съществени промени трябва да се извършва независим преглед на подхода на организацията за управление на сигурността на информацията и неговото прилагане (т.е. целите на контрола, механизмите за контрол, политиките, процесите и процедурите за сигурност на информацията).	
Чл.32(4) (сигурност на обработките) **Администратора и обработващия данни, ще осигурят, че техни служители ще работят с личните данни, единствено и само съгласно приетите инструкции.**	A.5.1.1 (политики за информационна сигурност) **Контрол** Трябва да бъде определен набор от политики за сигурност на информацията, одобрен от ръководството, разпространен и разгласен на всички служители и съответните външни страни. A.14.1.1 (анализ и спецификация на изискванията за сигурност на информацията) **Контрол** Изискванията, имащи отношение към сигурността на информацията, трябва да бъдат включени в изискванията за нови информационни системи или подобряване на съществуващи информационни системи. A.14.2.5 (принципи за сигурносх при системния инжинеринг) **Контрол** Инженерни принципи за сигурни системи трябва да бъдат създадени, документирани, поддържани и приложени при всеки опит за реализиране на информационна система.	**Препоръки** Политиките за информационна сигурност трябва да бъдат доразвити, чрез ясно деклариране, свързано с поддръжката и поемането на ангажименти за постигане на съответствие с приложимите изисквания за защита на личната информация, произтичащи от закон и/или договор между оператора на публичен „облак“, обработващ лични данни и съответния администратор (потребител науслугите по обработка на личните данни в „облака“) Съответния договор трябва да определи отговорностите на оператора на публичния „облак“ (обработващ данни) , неговите подизпълнители и потребителите на “облачни“ услуги (администратор), като се отчита типа на тези услуги – IaaS (инфраструктура, като услуга), PaaS (платформа, като услуга) или SaaS (софтуер, като услуга). Например, определянето на отговорностите за контроли по сигурността на приложно ниво, може да бъде различно, в зависимост дали се предоставят Saas, PaaS или IaaS услуги, на базата на които, администратора може да изгради собствени приложения, свързанис личните данни.
Чл.33 (1 и 3) (Уведомяване на надзорния орган за нарушение на сигурността на личните данни) **Администратора трябва да има процедури за управление на**	A.16.1.1 (Отговорности и процедури) **Контрол** Трябва да бъдат установени отговорности и процедури за управление, за да се осигури бърза, ефикасна и системна реакция на	A.9.1 Уведомяване за пробив в защитата на личната информация **Контрол** Опеартора на публичен облак, обработващ лична информация, трябва незабавно да уведоми своите потребители, в случай на

пробивите на защитата на личните данни, вкл за:уведомяване (в рамките на 72 ч.) на съответната агенция за защита на личните данни. **Уведомяването трябва да съдържа информация за:** **-типа та пролива;** **-категорията на личните данни;** **-броя субекти на данни;** **-номер на регистрацията;** **-данни за контакт със Служителя по защита на личните данни (ако е приложимо);** **-последствия за личните данни.**	инцидентите със сигурността на информацията. A.16.1.5 (Реакция на инциденти със сигурността на информацията) **Контрол** На инцидентите със сигурността на информацията трябва да се реагира в съответствие с документирани процедури. A.6.1.3 (Контакт с оторизираните органи) **Контрол** Трябва да се поддържат подходящи контакти със съответните оторизирани органи.	неупълномощен достъп до лична информация, ИТ техника, и /или помещения, довел до загуба, разкриване или подмяна на лични данни.
Чл.33 (5) (Уведомяване на надзорния орган за нарушение на сигурността на личните данни) Администратора трябва да събира и документира данни / информация (доказателства), свързани с възникнали пробивите на по сигурността)	A.16.1.7 (Събиране на доказателства) **Контрол** Организацията трябва да определи и прилага процедури за идентифициране,събиране, придобиване и съхраняване на информация, която може да послужи като доказателство. A.12.4 (Регистриране на събития) **Контрол** Трябва да бъдат изработвани, съхранявани и редовно извършвани прегледи на регистри за събития, записващи дейности на потребители, изключителни случаи, грешки и събития, свързани със сигурността на информацията.	**Препоръки** Регистъра на събития по сигурността (на оператора на публичен облак, обработващ и лични данни) трябва да бъде преглеждан периодично (съгласно напр., Инструкция за преглед), за да се установят нерегулярнеи дейности, с потенциал за нарушане на информационната сигурност. Регистрирането на събитията по сигурността, трябва да може да показва има ли засегната лична информация / данни, и ако има, кой е източника на съответното действие, и кога то е извършено. Оператора на публичен облак, който обработва лични данни трябва да определи критериите за предоставяне на данните от регистъра на събитията на своите потребители. За тази цел той трябва да има съответната процедура, с която да са запознати и съответните потребители.
Чл.33 (2) (Уведомяване на надзорния орган за нарушение на сигурността на личните данни) **Обработващия данни, разкрил пробив в сигурността на личните данни, веднага докладва на администратора за пробива.**	A.16.1.3 (Докладване за слабости в сигурността на информацията) **Контрол** Трябва да се изисква от служителите и доставчиците, използващи информационните системи и услуги на организацията, да отбелязват и докладват всяка наблюдавана или предполагаема слабост в сигурността в системите или	Няма допълнителен контрол

	услугите.	
Чл.34 (Съобщаване на субекта на данните за нарушение на сигурността на личните данни) Администратора ще оценява рисковете към субектите на данни, и ако тези рискове са с високи / неприемливи нива, то субетките на данни ще бъдат своевременно информирани.	A.16.1.5 (Реакция на инциденти със сигурността на информацията) **Контрол** На инцидентите със сигурността на информацията трябва да се реагира в съответствие с документирани процедури.	Няма допълнителен контрол
Чл.35 (1) (Оценка на въздействието върху защитата на данните) **Администратора решава дали да проведе оценка на въздействието върху защитата на данните, за съответен ИТ проект, като отчита обема и чувствителността на личните данни, целите на обработките и използваните технологии.**	A.6.1.5 (Сигурност на информацията при управление на проекти) **Контрол** Независимо от вида на проекта трябва да бъде отчетена сигурността на информацията при управление на проекти. A.14.1.1 (Анализ и спецификация на изискванията за сигурност на информацията) **Контрол** Изискванията, имащи отношение към сигурността на информацията, трябва да бъдат включени в изискванията за нови информационни системи или подобряване на съществуващи информационни системи. A.14.2.5 (Инженерни принципи за сигурни системи) **Контрол** Инженерни принципи за сигурни системи трябва да бъдат създадени, документирани, поддържани и приложени при всеки опит за реализиране на информационна система.	Няма допълнителен контрол
Чл.36 (1) (предварителни консултации) **Ако проведената оценка на въздействието върху защитата на личните данни показва високи нива на риск за субектите на данни, администратора трябва своевременно да уведоми за нова**	A.6.1.3 (Контакт с оторизираните органи) **Контрол** Трябва да се поддържат подходящи контакти със съответните оторизирани органи.	Няма допълнителен контрол

съответния надзорен орган.		
Чл.37 (Определяне на длъжностното лице по защита на данните) **Администратора и обработващия данни трябва да решат, дали ще определят конкретно лице, за изпълнение на задачи, свързани с постигането на съответствие с изискванията за защита на личните данни.**	А.6.1.1 (Роли и отговорности по сигурността на информацията) **Контрол** Трябва да бъдат определени и разпределени всички отговорности по сигурността на информацията	**Препоръки** Оператора на публичен облак, който обработва лични данни, трябва да оповести данни за контакт със своите потребители на услуги, свързани с обработката на лични данни по договор с тях.

Препоръки за изпълнение на изискванията по чл.24, 25, 28, 30, 32, 34, 35, 36, 37

Администратора е отговорен за изпълнението на изискванията на GDPR, свързани с обработките на личните данни. Това означава, че акоизискванията несе изпълняват, администратора може да бъде наказан и съществува риск да получи лоша „слава“ в обществото.
Администратора ще разработи политики и процедури, свързани с обработките на личните данни, а също и ще внедри съответните контролни / защитни механизми, доказващи практическото постигане на съответствие с изискванията на GDPR.
Това означава, че личните данни трябва да бъдат класифицирани и с тях да се работи, в съответствие разработените и прилагани процедури; че всички обработки налични данни са съответно документирани; че приложените мерки за сигурност са следствие от проведени оценка и анализ на риска; че сигурността е вградена в ИТ системите, още на ниво проектиране; че на пробивите н сигурността се реагира на база разработени процедури, инструкции, планове и др.; че, при необходимост е проведена оценка навъздействието върху защитата наличните данни; че е определено лице, изпълняващо функциите (както са описани в GDPR) на Служител по защитата на личните данни.

В GDPR са определени значителен брой директни задължения за обработващия данни. Както и администратора,той може да бъде наказан при неизпълнение на тези задължения.Отговорност на обработващия данни е да гарантира, че е внедрил подходящи технически и организационни мерки за сигурност, с цел защита на личните данни, които обработва. Освен това, той трябва да има и съгласието на администратора при договориране с подизпълнители на обработките (или на част от тях).

Забележка: След приемането на новия Закон за защита на личните данни, това ОР ще бъде своевременно актуализирано, както е приложимо.