McGregor & Partners

Going the extra mile

Commercial Lawyers

www.mcgregorlegal.eu

Предизвикателства за бизнеса относно защитата на личните данни – новия Европейски Регламент и Щит за неприкосновеността

Общ Регламент за Защита на Личните Данни

- 2012 г. – ЕК предлага Регламент относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (общ регламент относно защита на данните)
  - част от цялостна реформа на правилата за защита на личните данни - засилена защита за физическите лица и приспособяване към дигиталната ера
  - замества действащата досега Директива за защита на личните данни (95/46/ЕО), за да приложи еднакви правила навсякъде в ЕС
- Декември 2015 – институциите на ЕС постигат политическо споразумение относно текста на Общ Регламент ЗД
- 2016 – предстои окончателно приемане на Регламента от Европейския Парламент и Съвета и публикуване в Официалния вестник на ЕС
- 2018 – ефективно прилагане на новите правила

Как ще се отрази новия Общ Регламент ЗД на бизнеса

- Екстра-териториалност
- Засилена отговорност на администратора
- Мерки за постигане на съответствие
- Съгласие
- Прозрачност
- Санкции

Екстра-териториалност

- Общият Регламент ЗД ще се прилага и за администратори на лични данни, установени извън ЕС, които:
  - Предлагат стоки/ услуги на граждани на ЕС; или
  - Наблюдават поведението на граждани в ЕС
- „Наблюдение“: следене на лица в интернет за създаване на „профили“ с цел да се анализират или прогнозират техните лични предпочитания и поведение
- Сега действащите правила се прилагат за администратори извън ЕС, само ако използват средства за обработване разположени в ЕС
- Международни компании, които понастоящем локализират сървърите си извън ЕС и остават извън обхвата на Европейското законодателство за защита на личните данни, могат да попаднат в обхвата на Регламента ЗЛД, ако таргетират потребители в Европа
- Задължение за определяне на представител в ЕС; изключение: обработването няма вероятност да породи ***риск*** за правата и свободите на лицата
- Доколко ще е ефективно изпълнението на новите правила срещу администратори установени извън ЕС?

Засилена отговорност на администратора (Мерки за постигане на съответствие)

Принцип на **отчетност**: Въвеждане на подходящи технически и организационни мерки, за да се гарантира и да е в състояние да докаже, че обработването на лични данни се извършва в съответствие с Регламента

Мерки за постигане на съответствие:

1) **Поддържане на регистри на всички дейностите по обработване** в минимален обем посочен в Регламента

- Не е задължително за дружества с по-малко от 250 служители
- Но: изключението не важи ако има вероятност извършваното обработване да води до ***риск*** за правата и свободите на субекта на данни, обработването не е спорадично (occasional) или се обработват чувствителни данни

Засилена отговорност на администратора (Мерки за постигане на съответствие) 2

2) Оценка на въздействието върху защитата на личните данни

- предпоставка за обработването при **висок риск** то да засягане правата и свободите на физическите лица
- при мащабно обработване на чувствителни данни
- когато с автоматизирано обработване, включително „профилиране“ се оценяват лични аспекти (икономическо положение, местоположение, здравословно състояние, лични предпочитания) и въз основа на това се вземат решения, които пораждат последици или засягат значително лицето (напр. автоматичен отказ по онлайн заявление за кредит); публичен списък на операциите, които подлежат на оценка на въздействието ще се състави от контролния орган
- предварително консултиране с контролния орган преди обработването на лични данни, когато оценката на въздействието покаже висок риск, който администраторът не може да ограничи с подходящи мерки
- Понастоящем оценка на въздействие се изисква за всички администратори по действащата *Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни,* като следва да се извършва на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица. В зависимост от нивото на въздействие (от изключително високо до ниско) се определя и съответно ниво на защита, което представлява техническите и организационни мерки, които следва да осигури администраторът.

Засилена отговорност на администратора (Мерки за постигане на съответствие) 3

3) Определяне на лице, отговарящо за защитата на данните

- задължително само за компании, чиито ***основни*** *дейности се състоят от операции по обработване на лични данни*, които изискват: (i) редовно и систематично **наблюдение** на субекти на данни в големи мащаби (следят лицата с цел да анализират или предскажат личните им предпочитания) или (ii) обработване в големи мащаби на чувствителни лични данни (например данни отнасящи се до здравето)
- Лицето, отговарящо за защитата на данните може да бъде служител на компанията или външно нает, с експертиза в законодателството и практиката по защита на личните данни
- Задачи: да информира и консултира администратора за задълженията му, да наблюдава за съответствието с Регламента, да съдейства на контролния орган
- **Група предприятия** може да определи едно и също лице отговарящо за личните данни при условие, че е лесно достъпно от всяко дружество

Засилена отговорност на администратора (Мерки за постигане на съответствие) 4

4) Задължение за защита на данни още при проектирането („privacy by design“) и по подразбиране („privacy by default“)

- Защита на данните при проектиране - рискът за поверителност се взема предвид още в процеса на проектиране на нов продукт или услуга, като се предприемат подходящите технически и организационни мерки (например псевдонимизация) и процедури (например свеждане на данните до минимум) за съответствие с Регламента и защита на субектите на лични данни.
- Защита на данните по подразбиране – обработване по подразбиране само на данни, които са необходими за всяка конкретна цел, т.е. данните не се събират или запазват в обем или за срок на съхранение, по-голям от минимално необходимия за тези цели. По подразбиране личните данни не са достъпни за неограничен брой физически лица.

Засилена отговорност на администратора (Мерки за постигане на съответствие) 5

5) Уведомяване на контролния орган при нарушения на лични данни

- Уведомяване на органа в случай на нарушение на сигурността на личните данни не по-късно от 72 часа след установяването му
- Освобождаване от уведомяване: ако нарушението не би довело до риск за правата и свободите на физическите лица. Широко формулирани рискове от нарушения.
- Препоръчително уведомяване във всички случаи на съмнение за нарушение.
- Уведомяване и на субектите на лични данни за нарушението, когато то би довело до висок риск за тяхната неприкосновеност

6) Кодекси на поведения и Сертифициране

- Кодекси - одобрени от контролния орган/ ЕК
- Сертифициране от акредитиран орган; печати и маркировки за защита на данните
- Ограничават риска на администратора - елемент за доказване за съответствие с Регламента

Законосъобразно обработване

Условията за законосъобразно обработване съответстват на сегашната регулация:

- **съгласие на субекта** за една или повече конкретни цели
- **договор,** по който субектът на данните е страна
- **законово задължение** спрямо администратора
- защита жизненоважните интереси на субекта на данните или на друго физическо лице
- изпълнение на обществен интерес или упражняването на законови правомощия на администратора
- необходимо за целите на **законните интереси** на администратора или на трето лице

Съгласие

*„Свободно изразено, конкретно, информирано и **недвусмислено** указание за волята на субекта на данните,*

*посредством изявление или **ясно потвърждаващо действие**, което изразява съгласието му свързаните с него лични данни да бъдат обработени“*

- Нови изисквания за администраторите: да получат **недвусмислено съгласие** чрез **ясно потвърждаващо действие**
- Няма да е валидно „подразбиращото се съгласие“ – например, самото използване на уебсайт в който потребителят се е съгласил мълчаливо с безкрайни общи условия, част от които е съгласието за обработване; маркирано отнапред съгласие от администратора; неизвършване на действия от потребителя (непроменяне на настройките за сигурност)
- Съгласието трябва да гарантира информираност на лицето за това, че дава съгласието си и точно за какво го дава
- Получаването на съгласие в контекста на договор: не може да се изисква, като условие да се даде достъп до услуга, когато личните данни не са необходими за изпълнението на договора.
- Оттегляне на съгласието – възможност по всяко време; да е толкова лесно да оттеглиш, колкото и да изразиш съгласие (т.е. при същите условия).
- Изрично съгласие за обработване на чувствителни лични данни

Прозрачност

Администраторите на лични данни са длъжни да представят значителен обем информация на лицата, чийто данни обработват:

- **към момента на получаване на данните** – в допълнение на сега изискваната информация за идентификация на администратора, целите на обработване, получателите на които може да се разкрие, правото на достъп и правото на коригиране, още и следната информация:
- срока, за който ще се съхраняват личните данни, или ако не е възможно критериите по които се определя
- съществуването на редица права на лицата, включително: за заличаване на данните („да бъде забравен“), за ограничаване или възразяване срещу обработването, право на преносимост на данни (да получи данните в електронен формат за по-нататъшното им използване от друг администратор), право да оттегли съгласието си (когато обработването е въз основа на такова) и право на жалба до контролиращия орган
- дали предоставянето на лични данни е на законово или договорно изискване, или предпоставка за сключване на договор, и дали лицето е длъжно да предостави данните и последиците ако не ги предостави
- съществуването на обработване чрез профилиране и информация за използваната логика и значението и последиците от това обработване за лицето.
- при намерение за допълнително обработване за цел, различна от тази, за която са събрани – предварителна информация за въпросната друга цел и всякаква друга необходима информация

Новите правилата отговарят до голяма степен на сегашните добри практики в политиките за поверителност на компаниите, но е необходим внимателен анализ за съответствие и адаптиране при необходимост.

Санкции

- Регламент ЗЛД предвижда значително високи санкции в сравнение с прилаганите в момента по местните законодателства в ЕС.
- При нарушения на действащия в момента Закон за защита на личните данни, санкциите са от 10 000 лв. до 100 000 лв.
- Двустепенна система на санкции съгласно Регламент ЗЛД:

- До **EUR 10 000 000 или 2 %** от годишния **световен оборот** на предприятието за предходната финансова година (която сума е по-висока) - за по-леки нарушения на административни разпоредби на Регламента, например ако не е водена документация за всички операции по обработване, не е уведомен контролния орган за нарушения на лични данни, не е извършена оценка за въздействие, не е назначен служител за защита на личните данни
- До **EUR 20 000 000 или 4 %** от годишния **световен оборот** на предприятието за предходната финансова година (която сума е по-висока) - за фундаментални нарушения, например на основните принципи за обработване на данните, включително условията за съгласие (когато обработването е въз основа на такова), на правата на субектите на лични данни, на правилата за трансфери на получатели в трети страни

Годишния световен оборот – на юридическото лице извършило нарушението или на групата предприятия? Регламент ЗЛД препраща към „предприятие” съгласно чл. 101 и 102 от ДФЕС.

- **Значително се повишава риска на бизнеса при несъответствие със законодателството за защита на личните данни.**
- **Необходим е критичен преглед на политиките и практиките на компаниите за защита на личните данни преди влизане в сила на Регламент ЗЛД.**

Щит за личните данни (EU-U.S. Privacy Shield)

- Решението Schrems
- Алтернативни решения
  - Договорни клаузи
  - Задължителни фирмени правила
- Щит за личните данни
- Проблеми

Решение Schrems (C-362/141) 6 октомври 2015

- Отменя *Принципите за „Сфера на неприкосновеност на личния живот" (Safe Harbour),* приети с Решение на ЕК (2000/520/ЕО), гарантиращи адекватността на защитата на личните данни на територията на САЩ
- Приема, че правото на защита на личните данни, гарантирано от Хартата на основните права на ЕС не може да бъде засегнато чрез отмяна/намаляване на правомощията, с които разполагат националните надзорни органи
- Дори при наличие на решение на ЕК *(Safe Harbour)*, националните надзорни органи, до които е отправено искане, трябва да могат напълно независимо да проверят дали прехвърлянето на лични данни на определено лице към трета страна отговаря на европейското законодателство

Решението Schrems 2

- В Решение Shrems съдът установява, че:
  - ✓ схемата се прилага само за присъединилите се към нея американски предприятия, като самите публични органи на САЩ не са длъжни да я съблюдават
  - ✓ изискванията, свързани с националната сигурност, с обществения интерес и със спазването на законодателството на САЩ се ползват с предимство пред Safe Harbour, така че американските предприятия са длъжни без ограничения да се отклоняват от предвидените в Safe Harbour правила за защита, когато последните влизат в противоречие с въпросните изисквания.
- Въз основа на всички тези съображения Съдът обявява рамката Safe Harbour за невалидна
- Предаването на данни между ЕС и САЩ вече не може да се извършва на основание Safe Harbour
- Safe Harbour така или иначе не се прилагаше от КЗЛД (Становище от 30.09.2015 г.) - прехвърлянето на данни на основание Safe Harbour подлежи на разрешителен режим

Алтернативни решения

- Алтернативни основания за предаване:
  - Стандартни договорни клаузи, изготвени от Комисията
  - Задължителни фирмени правила— по отношение на предаване на данни между различните субекти в рамките на мултинационална корпоративна група

Стандартни Договорни клаузи

- Четири набора от СДК одобрени от ЕК- изпълняват изискванията за достатъчни гаранции по Директивата. Два набора от стандартни клаузи се отнасят до предаването на данни между администратори, другите два касаят предаването между администратора и обработващия лични данни, действащ по негови указания
- Включването на СДК в договор води до това, че националните органи, по принцип, са задължени да ги приемат
- Българско законодателство и практика - трансферът на лични данни до САЩ без да се иска разрешение от КЗЛД (уведомителна процедура), е възможен при сключването на договор при стандартните клаузи. Ако обаче администраторите на лични данни не желаят поемането на предвидените в стандартните клаузи задължения, те ще могат да разчитат на по-тежката процедура по искане на разрешение за трансфер.

Задължителни фирмени правила

- Многонационалните дружества могат да приемат задължителни фирмени правила за предаване на лични данни от ЕС на свързани предприятия от групата, разположени извън ЕС; основание за предаване на данни само в рамките на дадена корпоративна група
- Използването на ЗФП позволява личните данни да се движат свободно между различните субекти, които са част от дадена корпоративна група на световно равнище
- Практика на КЗЛД - предоставянето на лични данни на основание ЗФП в трета държава се извършва след разрешение на КЗЛД, която преценява адекватността на защита
- Новия Общ Регламент ЗД – признава ЗФП изрично като основание; следва да се прилага уведомителен режим

Щит за личните данни (EU-U.S. Privacy Shield)

Февруари 2016 - ЕК публикува проект на нова рамка за трансатлантическите трансфери на данни между ЕС и САЩ **„Щит за личните данни в отношенията между ЕС и САЩ (“EU-U.S. Privacy Shield**”). Новата рамка следва да осигури адекватно ниво на защита на личните данни, предавани от ЕС на САЩ. „Щитът” се състои от принципи, които дружествата приемат да спазват, включително писмени ангажименти от правителството на САЩ.

Ключови изисквания:

- Годишно самосертифициране и включване в списъка на дружествата, приели Privacy Shield; постоянен обект на контрол от страна на Департамента по търговия в САЩ; санкции при неспазване на принципите; задължение за публикуване на политиката на дружествата за защита на личните данни
- Ясни гаранции и задължения за прозрачност във връзка с достъпа на държавните органи на САЩ до лични данни: САЩ поемат ангажимент да ограничат достъпа на държавните си органи до лични данни, когато те се обработват за целите на правоприлагането и националната сигурност, като ще се въведат ясни ограничения, гаранции и механизми за надзор

Щит за личните данни 2

- Ефективна защита на правата на гражданите на ЕС с няколко възможности за правна защита: разглеждане на жалби в срок от самите дружества, подаване на жалби срещу американски компании в националните органи за защита на личните данни и препращането им до компетентните американски органи, безплатна възможност за алтернативно разрешаване на спорове, арбитражен механизъм, чието решение е задължително и изпълнимо срещу американско дружеството, създаване на независим омбудсман и дори пряк достъп на европейските граждани до американските съдилища
- Механизъм за извършване на годишен съвместен преглед; чрез този механизъм ще се осъществява мониторинг върху функционирането на Щита за личните данни, включително и за съблюдаването на ангажиментите и уверенията относно достъпа до данните за целите на правоприлагането и националната сигурност. В случай, че се установят нарушения, действието на “Щита” може да бъде преустановено
- Предстои ЕК да приеме решение, че САЩ осигурява адекватно ниво на защита на личните данни чрез EU-U.S. Privacy Shield – юни 2016 г.?

Проблеми

- Ще бъдат ли изпълнени поетите задължения по Privacy Shield?
- Ще бъдат ли ефикасни и действащи въведените механизми за контрол?
- Дали сегашното законодателство на САЩ е в състояние да осигури необходимите гаранции за защитата на личните данни на европейските граждани?
- КЗЛД ще признае ли адекватно ниво на защита, когато трансфер до САЩ се извършва на основание Privacy Shield, без да е необходима разрешителна процедура?

Благодаря!

Контакти:

Юлиан Спасов

julian.spassov@mcgregorlegal.eu

Ася Владимирова

asya.vladimirova@mcgregorlegal.eu

+359 (2) 865 17 17

София, бул. Христо Смирненски 11

McGregor & Partners
BUCHAREST & SOFIA