I.Въведение

Регламента за защита на личните данни (ЕС) 2016/679 (GDPR) на Европейския парламент и на Съвета на Европа от 27 април 2016г. за защита на физическите лица при обработване на лични данни и за свободно движение на такива данни и за отмяна на Директива 95/46/ЕО има пряко действие за държавите – членки, считано от 25.05.2018г. Неговата цел е да уеднакви политиките на държавите-членки на ЕС по отношение на начина за събиране и използване на лични данни, както и да осигури възможност за свободно движение на данни в рамките на цифровия единен пазар, както и да гарантира по-добра защита на неприкосновеността на личния живот.

Обхват

Материален обхват - Регламента (ЕС) 2016/679 се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни (ръчно и на хартия), които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни.

Териториален обхват - Регламента (ЕС) 2016/679 се прилага за всички администратори на лични данни, които са установени в ЕС, които обработват лични данни на физически лица, в контекста на своята дейност. Ще се прилага и за администратори извън ЕС, които обработват лични данни с цел да прилагат стоки и услуги или ако наблюдават поведението на субектите на данни, които се намират в ЕС.

1. Понятия

„Лични данни“ - всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци , специфични за физическата, физиологичната , генетичната, психическата, умствената, икономическата или социална идентичност на това физическо лице.

„Специални категории лични данни“ – лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации и обработката на генетични данни, биометрични данни за уникално идентифициране на физическо лице, данни отнасящи се до здравето или данни относно сексуалния живот или сексуалната ориентация на физическото лице;

„Данни за здравословното състояние“- означава лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние;

„Обработване“ - означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване организиране, структуриране, съхраняване, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване или комбиниране, ограничаване, изтриване или унищожаване;

„Администратор“ – всяко физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определи целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на ЕС или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на държава членка;

„Обработващ“ - всяко физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

„Субект на данните“ - всяко живо физическо лице, което е предмет на личните данни обработвани от администратора;

„Съгласие на субекта на данните“ – всяко 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;

„Регистър с лични данни“ означава всеки структуриран набор от лични данни , достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

„Профилиране“ - всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитани, интереси, надеждност, поведение, местоположение или движение;

„Нарушение на сигурността на лични данни“ – нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

„Получател“ – физическо или юридическо лице, публичен орган, агенция или друга структура , пред която се разкриват личните данни, независимо дали е трета страна или не;

„Трета страна“ – всяко физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващ лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

„Надзорен орган“ – означава независим публичен орган, създаден от държава членка съгласно член 51/4.5.2016г. За България надзорен орган е Комисия за защита на личните данни.

II. Декларация за ангажираност относно политиката за неприкосновеност на личните данни

1. Комисията за регулиране на съобщенията се ангажира да осигури съответствие със законодателството на ЕС и с националното законодателство по отношение на обработването на личните данни и защитата на правата и свободите на лицата, чийто лични данни комисията събира и обработва съгласно Регламента (ЕС)2016/679.
2. В съответствие с Регламента към настоящата политика са описани и други релевантни документи, както и свързани протоколи и процедури.
3. Регламента (ЕС) 2016/679 и настоящата политика се отнасят до всички функции по обработването на лични данни, включително тези, които се извършват относно лични данни на служители, стажанти, клиенти, доставчици и партньори и до всякакви други лични данни, които комисията събира от различни източници.
4. Длъжностното лице по защита на данните отговаря за преразглеждането на Регистъра на дейностите по обработване, както и всички допълнителни изисквания, оценки на риска относно защитата на данните
5. Тази политика се прилага за всички служители и стажанти. Всяко нарушение на Регламента (ЕС)2016/679 ще бъде разглеждано като нарушение на трудовата дисциплина, а в случай че има предположение за извършено нарушение, въпросът своевременно ще се предостави за разглеждане на компетентните държавни органи.

III. Система за управление на лични данни (СУЛД)

1. За да се спази принципа на Отчетност от Регламента (ЕС) 2016/679 Председателя на Комисията за регулиране на съобщенията одобри актуализирането и усъвършенстването на Системата за управление на лични данни (СУЛД).

Всички служители на КРС и определени външни лица, идентифицирани в СУЛД е необходимо да спазват тази политика. Последствията от нарушаването на тази политика са изложени във Вътрешната процедура за действията, които се предприемат във връзка с нарушения на сигурността на личните данни, обработвани от Комисията за регулиране на съобщенията и нейната администрация;

2. При определянето на обхвата си за съответствие с Регламента (ЕС)2016/679 КРС е съобразила и отчела потенциалното влияние на :
   - Всякакви външни и вътрешни предизвикателства, които са свързани с целите на КРС и които влияят върху нейната способност да постига желаните резултати от своята Система за управление на лични данни (СУЛД);

- Организационните цели и задължения;
- Всички приложими законови, регулаторни или договорни задължения.

Целите на КРС за спазване на СУЛД :

- са в съответствие с тази политика;
- вземат под внимание Регламента (ЕС)2016/679 и резултатите от оценката на риска;
- се актуализират според необходимостта.

За да постигне тези цели КРС предприе:

- актуализиране на действащата СУЛД ;
- какви ресурси ще бъдат необходими.

IV. Задължения и роли по Регламента (ЕС)2016/679

1. Комисията за регулиране на съобщенията е администратор на данни, а в някои случаи и обработващ данни по смисъла на Регламента (ЕС)2016/679.
2. Комисията за регулиране на съобщенията е отговорна за актуализиране и разработване процедури за гарантиране защитата на личните данни.
3. Длъжностното лице по защита на данните (ДЛЗД) (с роля и задължения, посочени в Чл. 37-39 от Регламента (ЕС)2016/679 и длъжностната му характеристика) се отчита на Председателя на КРС за управлението на лични данни в рамките на компанията и за гарантирането на възможността за доказване на съответствието със законодателството за защита на данните и добрите практики.
   Тази отчетност на ДЛЗД включва:
   - Разработване и актуализиране на вътрешно-организационни документи за спазване на изискванията на Регламента (ЕС)2016/679 ;
   - Управление на сигурността и риска по отношение на съответствието с политиката.
4. ДЛЗД носи отговорност за съответствието на КРС с настоящата политика. ДЛЗД съдейства на комисията да гарантира, че дейността на КРС и дейността на всеки служител, която се извършва в рамките на неговата област на отговорност, съответстват на изискванията на Регламента (ЕС)2016/679.
5. ДЛЗД има отговорности и е необходимо да разяснява процедурите, както процедурата за взаимодействие със субектите на лични данни за служителите на организацията и потребителите на услугите.
6. Спазването на законодателството за защита на данните е отговорност на всички служители на КРС, които обработват лични данни.
7. Политиката за обучение на КРС определя специфичните изисквания за обучение и осведомяване във връзка с конкретните роли на служителите на комисията .

V. Принципи за защита на данните

Обработката на лични данни се извърши в съответствие с принципите за защита на данните, посочени в Член 5 от Регламента (ЕС)2016/679. Политиките и процедурите на КРС имат за цел да гарантират спазването на тези принципи.

1. Личните данни трябва да бъдат обработвани законосъобразно, добросъвестно и прозрачно

Законосъобразно – да идентифицира правно основание преди да обработва лични данни („основания за обработване“) ;

Добросъвестно – за да може обработването да бъде добросъвестно, администраторът на данни трябва да предостави определена информация на субекта на данни, доколкото това е практически възможно. Това важи независимо дали личните данни са получени директно от субектите на данни или други източници;

Прозрачност - Регламента (ЕС)2016/67 включва правила относно предоставяне на подробна информация на субектите на данни. Те са подробни и конкретни, поставяйки акцента върху това, че уведомленията за поверителност са разбираеми и достъпни. Информацията трябва да бъде съобщена на субекта на данни в разбираема форма, като се използва ясен и разбираем език.

Специфичната информация, която трябва да бъде предоставена на субекта на данните, трябва да включва като минимум:

- Идентичност и данни за контакт на администратора;
- Идентичност и данни за контакт на ДЛЗД;
- Цел и правно основание за обработването;
- Дали предоставянето на лични данни е част от законово или договорно изискване или задължение и евентуално последици от непредоставянето им;
- Легитимните интереси на администратора или трета страна, когато е приложимо;
- Категориите лични данни;
- Периода, за който ще се съхраняват личните данни или критерии, използвани за определянето му;
- Съществуването на следните права – да поиска достъп до данните, коригиране, изтриване (право „да бъдеш забравен“), ограничаване на обработването, както право на възражение;
- Правото да оттегли съгласието, когато е приложимо;
- Право на подаване на жалба;
- Получателите или категориите получатели на лични данни, когато е приложимо;
- Дали администраторът възнамерява да прехвърли личните данни към получател в трети страна и нивото на защита на данните;

- Всякаква допълнителна информация, необходима да се гарантира добросъвестно обработване.

2. Лични данни могат да се събират само за конкретни, изрично указани и законови цели Данните, получени за конкретни цели, не трябва да се използват за цел, която се различава от тези, официално обявени на надзорния орган като част от Регистъра на дейностите по обработване на данни по Чл. 30 от Регламента (ЕС)2016/679.

3. Личните данни трябва да бъдат адекватни, релевантни, ограничени до това, което е необходимо за обработването им със съответната цел (принцип на минимално необходимото).
   - Всички формуляри за събиране на данни (електронни или на хартиен носител), включително изискванията за събиране на данни в СУЛД, трябва да включват уведомление за поверителност и да бъдат съгласувани с ДЛЗД;
   - ДЛЗД ще гарантира, че ежегодно всички способи за събиране на данни се преглеждат от него, за да се гарантира, че събраните данни ни не са прекомерни . Извършва се процедура за оценка на риска .

4. Личните данни трябва да бъдат точни и актуализирани във всеки един момент и да са положени необходими усилия, за да е възможно незабавно (в рамките на възможните технически решения) изтриване или коригиране.
   - Данните, които се съхраняват от администратора на данни, трябва да бъдат прегледани и актуализирани при необходимост.
   - ДЛЗД е отговорно да гарантира , че всички служители са обучени в значението за събирането, обработването и съхранението им.
   - Също така, задължение на субекта на данните е да декларира, че данните, които предава за обработване на КРС са точни и актуални.
   - От служителите, изпълнителите по граждански договори, клиентите, партньорите и др. трябва да се изисква, да уведомяват КРС за всякакви промени в обстоятелствата, за да могат да се актуализират записите на лични данни. Отговорност на КРС е да гарантира, че всяко уведомление относно промяната на обстоятелствата е записано и се предприемат действия.
   - ДЛЗД носи отговорност да се гарантира, че са налице подходящи процедури и политики за поддържане на точни и актуални лични данни.
   - ДЛЗД ежегодно преглежда сроковете на съхранение на всички лични данни, обработвани от КРС, като се позовава на инвентаризацията на данните и ще идентифицира всички данни, които вече не се изискват. Тези данни ще бъдат надеждно унищожени в съответствие с процедурите и правилата на администратора.
   - ДЗЛД е отговорен за прилагането на подходящи мерки при взаимодействие с трети страни (обработващи), когато данните са неточни или неактуални, да ги информира, както и за предаването на всяка корекция на лични данни на трета страна, когато това се изисква.

5. Личните данни трябва да се съхраняват в такава форма, че субектът на данните може да бъде идентифициран само толкова дълго, колкото е необходима за обработването.
   - Когато личните данни се спазват след дата на обработването, те ще бъдат съхранявани по подходящ начин (анонимизирани, криптирани, псевдонимизирани), за да се защити самоличността на субекта на данните в случай на нарушение на данните.
   - Лични данни ще бъдат пазени в съответствие с процедура за съхраняване и унищожаване на данните и след като е преминал срокът им на съхранение, те ще бъдат надлежно унищожени по указания начин.
   - ДЗЛД трябва писмено да одобри всяко запазване на данни, което надхвърля срока на съхранение, дефиниран в процедурата за съхраняване и унищожаване на данните и трябва, да гарантира , че обосновката е ясно определена и е в съответствие с изискванията на законодателството за защита на данните.
6. Личните данни трябва да бъдат обработени по начин, който гарантира подходяща сигурност.
7. ДЗЛД ще извърши оценка на риска съблюдавайки Политиката за мрежова и информационна сигурност в КРС, като вземе предвид всички обстоятелства, свързани с операциите по управление или обработване на данни .

При оценяването на подходящи технически мерки, ДЛЗД разгледа следното, за да предложи мерки за утвърждаване от администратора:

- Защита с парола;
- Автоматично заключване на бездействащи работни станции в мрежата;
- Премахване на права на достъп за USB и други преносими носители с памет;
- Антивирусен софтуер и защитни стени;
- Права за достъп, основани на роли, включително на назначен временно персонал;
- Защитата на устройства, които напускат помещенията на организацията, като лаптопи или други;
- Сигурност на локални мрежи;
- Технологии за подобряване на поверителността, като например псевдоминимизиране и анонимизиране;

При оценяването на подходящите организационни мерки ДЛЗД взема предвид следното, за да предложи подходящи мерки за утвърждаване от КРС:

- Нивата на подходящо обучение в КРС;
- Мерките, които отчитат надеждността на служителите (например атестационни оценки, препоръки и т.н.);
- Включването на защитата на данните в трудовите договори;
- Идентификация на предвидени мерки за нарушение по отношение на обработването на данни;

- Редовна проверка на персонала за спазване на съответните стандарти за сигурност;
- Контрол на физическия достъп до електронни и хартиено базирани записи;

- Приемане на правила за „чисто работно място“;
- Съхраняване на хартия на базата данни в заключващи се шкафове;
- Ограничаване на използването на портативни електронни устройства извън работното място;
- Приемане на ясни правила за създаване и ползване на пароли;
- Редовно създаване на резервни копия на личните данни и физическо съхраняване на носителите с копия;
- Налагане на договорни задължения на организации, партньори, контрагенти да предприемат подходящи мерки за сигурност при прехвърляне на данни извън ЕС.

8. Спазване на принципа на отчетност

Регламента (ЕС)2016/679 включва разпоредби, които насърчават отчетността и управляемостта и допълват изискванията за прозрачност. Принципът на отчетност изисква от администратора да докаже, че спазва принципите в Регламента (ЕС)2016/679 и изрично заявява, че това е негова отговорност.

КРС доказва спазването на принципите за защита на данните чрез прилагане на политики по защита на данните, като се присъединява към вътрешните правила, внедрява подходящи технически и организационни мерки, както и чрез приемане на техники по защита на данните на етапа на проектиране и защита на данните по подразбиране, оценка на съответствието за защита на личните данни.

VI. Процедура по обработка на лични данни

1.Обхват

Цялата обработка на лични данни от КРС е в обхвата на тази процедура.

2. Отговорности

2.1 КРС изпълнява ангажимента на администратора, да публикува Политиката за поверителност на електронната страница на комисията и уведомленията за поверителност за различни категории лица, които да гарантират, че всички субекти на данни са получили информацията, изискуема съгласно Регламента (ЕС)2016/679 преди началото на събирането от комисията на данни.
2.2. Всички служители, които извършват събиране на лични данни, трябва да следват тази процедура.

3.Процедура

3.1. КРС извършва операции по обработка, като ясно се определени, дефинирани и документирани:

3.1.1.конкретната цел на обработката на лични данни;

3.1.2.правното основание за обработката на лични данни:

3.1.2.1.съгласие, получено от субекта на данните;

3.1.2.2.изпълнение на договор, по който субектът на данни е страна;

3.1.2.3.законова задължение, което КРС трябва да изпълни;

3.1.2.4.защитата на жизненоважни интереси на субекта на данните, включително защитата на правата и свободите;

3.1.2.5.изпълнение на задача от обществен интерес,

3.1.2.6.легитимни интереси на администратора на данни или на трета страна;

3.1.3.всички специални категории обработени лични данни и правното основание за обработка на данните съгласно:

3.1.3.1.изрично съгласие, получено от субекта на данните;

3.1.3.2.необхидими за трудови права или задължения;

3.1.3.3.защита на жизненоважните интереси на субекта на данните, включително защитата на правата и свободите;

3.1.3.4.необходими за законни дейности с подходящи гаранции и е свързано единствено с членовете на КРС;

3.1.3.5.лични данни, направени публично достояние от субекта на данните;

3.1.3.6.правни рискове;

3.1.3.7.важен обществен интерес на основание правото на Съюза или на държава-членка;

3.1.3.8.превантивна или трудова медицина, за оценка на трудоспособността на служителя, медицинска диагноза, предоставяне на здравни или социални грижи или лечение, въз основа на които са сключени договори със здравни специалисти и съществуват предпазни мерки;

3.1.3.9.архивиране в обществен интерес, за научни или за статистически цели.

4.Уведомления за поверителност

4.1. Когато се събират лични данни със съгласието на субекта на данните КРС е прозрачна при обработката на лични данни и предоставя на субекта на данни

уведомления зя поверителност по образец на различни групи субекти, съдържащи информация, посочена в чл.13 от Регламента (ЕС)2016/679 .

4.2.Когато данните се изискват по договор КРС обработва данни за изпълнение на договорни задължения при осигуряване на наличието на адекватни договорни клаузи в договора.

4.3.Когато лични данни са получени от източник, различен от субекта на данните КРС изяснява видовете събрана информация, както и източника на лични данни (публично достъпни източници) и предоставя на субекта на данни информацията, посочена в чл.14 от Регламента (ЕС)2016/679 .

4.4. Чл.4.1. и чл.4.3 по-горе не се прилагат, ако субектът на данните вече разполага с информацията.

4.5 Чл.4.3. по-горе не се прилага, ако предоставянето на такава информация се окаже невъзможно или изисква несъразмерно големи усилия.

5.Предоставяне на информация

5.1.КРС предоставя информация, посочена в чл.4.1 и чл.4.3 по-горе, в рамката на:

5.1.1. по чл.4.1. – към момента на събиране на данните;

5.1.2.по чл.4.3. – в срок от един месец от получаване на личните данни в съответствие със специфичните обстоятелства на обработката; ако данните се използват за комуникация с лицето, най-късно при първата комуникация; ако се предвижда разкриване пред друг получател, най-късно преди данните да бъдат оповестени.

VII. Права на субекта на данни

1. Субекта на данни има следните права по отношение на обработването на негови лични данни, свързани с него, и ако това е така, да получи достъп до данните, както и информация кои са получателите на тези данни;
   - Да отправя искания за потвърждаване дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните, както и информация кои са получателите на тези данни;
   - Да поиска копие от своите лични данни от администратора;
   - Да поиска от администратора коригиране на лични данни, когато те са неточни, както и когато не са вече актуални;
   - Да поиска от администратора изтриване на лични данни (право „да бъдеш забравен“) при определените за това условия;
   - Да иска от администратора ограничаване на обработването на лични данни, като в този случай данните ще бъдат само съхранявани, но не и обработвани;
   - Да направи възражение срещу обработване на негови лични данни;

- Да направи възражение срещу обработване на лични данни, отнасящи се до него за целите на директен маркетинг;
- Да се обърне с жалба до Комисията за защита на личните данни (КЗЛД), ако смята, че някоя от разпоредбите на Регламента (ЕС)2016/679 е нарушена;
- Да поиска да му бъдат предоставени личните данни в структуриран, широко използван и пригоден за машинно чете формат;
- Да оттегли съгласието си за обработката на личните данни по всяко време с отделно искане, отправено до администратора, ако основанието за обработване е съгласие;
- Да не обект на автоматизирано взети решения, които да го засягат в значителна степен, без възможност за човешка намеса;
- Да се противопостави на автоматизирано профилиране, което се случва без негово съгласие.

2. КРС е осигурила условия, които да гарантират упражняването на тези права от субекта на данни:
   - Субектите на данни могат да направят искания за достъп до данни, както е описано в Процедурата за заявка до достъп до данните, която описва как КРС гарантира, че отговора на искането на субекта на данни отговаря на изискванията на Регламента (ЕС)2016/679.
   - Субектите на данни имат право да подават жалби до КРС, свързани с обработването на личните им данни и обработването на техните искания в съответствие с Процедурата за жалби.

VIII. Съгласие

1. Под „съгласие" КРС разбира всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните него лични данни да бъдат обработени. Субектът на данните може да оттегли своето съгласие по всяко време.

2. КРС разбира под „съгласие" само случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие и без върху него да бъде упражняван натиск. Съгласието, получени при натиск или въз основа на подвеждаща информация не е валидно основание за обработване на лични данни.
3. Съгласието не може да бъде изведено от липса на отговор на съобщение до субекта на данни. Трябва да има активна комуникация между администратора и субекта, за да е налице съгласие. Администраторът трябва да може да докаже, че е получено съгласие за дейностите по обработване чрез уведомление за поверителност или формуляр за съгласие.

4. За специални категории данни трябва да се получи изрично писмено съгласие на субектите на данни, освен ако не съществува алтернативно законно основание за обработване.

IX. Сигурност на данните

1. Всички служители са отговорни за гарантирането на сигурността при съхраняването на данните, за които те отговарят и които КРС държи, както и, че данните се съхраняват сигурно и не се разкриват при каквито и да било обстоятелства на трети страни, освен ако (компанията) не е дала такива права на тази трета страна, като е сключила договор Администратор-Обработващ или става дума за държавен орган с посочена от закона компетентност да изисква такива данни.
2. Всички лични данни трябва да бъдат достъпни само за тези, които се нуждаят от тях, а достъпът може да бъде предоставен само в съответствие с Процедурата за контрол на достъпа. Всички лични данни трябва да се третират с най-голяма сигурност и трябва да се съхраняват:
    - в стая с контролиран достъп и/или в заключен шкаф или в картотека и/или
    - ако са компютъризирани – да са защитени с парола в съответствие с вътрешните изисквания посочени в организационните и технически мерки за контролиране на достъпа до информация.

3. Да се създаде организация, която да гарантира, че компютърните екрани и терминалите не могат да бъдат гледани от друг, освен от оторизираните служители на КРС. От всички работници/служители се изисква да бъдат обучени и да приемат съответните договорни клаузи/декларации за спазване на организационните и технически мерки за достъп, както и правилата за заключване на работните станции, преди да им бъде предоставен достъп до информация от всякакъв тип.
4. Записите върху хартиен носител не трябва да се оставят там, където могат да бъдат достъпни от неоторизирани лица и не могат да бъдат изваждани от определените офисни помещения без изрично разрешение. Веднага щом хартиените документи вече не са необходими за текущата работа, те трябва да бъдат унищожени съответствие със създадена за това процедура.
5. Личните данни могат да бъдат изтривани или унищожавани само в съответствие с Процедурата за съхраняване и унищожаване на данни. Записите на хартиен носител, които са достигнали крайната дата на съхранение, трябва да бъдат нарязани и унищожени като „поверителни отпадъци“. Данните върху твърдите дискове на неизползвани или бракувани персонални компютри и записващи носители трябва да бъдат изтрити или дисковете унищожени, съгласно изградените правила чрез изтриване или унищожаване на самите носители.
6. Обработването на лични данни „извън офиса“ представлява потенциално по-голям риск от загуба, кражба или нарушение на сигурността на личните данни.

Работниците/служителите/изпълнителите по граждански договори трябва да бъдат специално упълномощени да обработват данните извън обекта на администратора.

X. Разкриване на данни

1. КРС трябва да осигури условие, при които личните данни не се разкриват на неупълномощени трети страни, което включва членове на семейството, приятели, държавни органи, дори разследващи такива, ако има основателно съмнение, че не се изискват по установения ред. Всички служители трябва да бъдат предпазливи, когато им поискат да разкрият съхранявани лични данни за друго лице на трета страна. Важно е да се има предвид, дали разкриването на информацията е свързано или не с нуждите на дейността, извършвана от организацията.

Необходимо е на служителите да се извърши специално обучение и периодични инструктажи с цел да се избегне рискът от такова нарушение.

2.Всички искания от трети страни за предоставяне на данни трябва да бъдат подкрепени с подходяща документация и всички такива разкривания на данни трябва да бъдат специално разрешени от ДЛЗД.

XI. Съхраняване и унищожаване на данните

1. КРС не съхранява лични данни във вид, който позволява идентифицирането на субектите за по-дълъг период отколкото е необходима, по отношение на целите, за които са били събиране данните.

2. КРС може да съхранява данни за по-дълъг период единствено, ако личните данни ще бъдат обработвани за целите на архивиране, за цели в обществен интерес, научни или исторически изследвания и за статистически цели, и само при изпълнение на подходящи технически и организационни мерки за гарантиране на правата и свободите на субекта на данните.

3.Периодът на съхранение за всяка категория на лични данни, както и критериите, използвани за определяне на този период, включително всякакви законови задължения в тази връзка, са посочени в Процедурата за съхраняване и унищожаване на данните и графика към нея.

4.личните данни трябва да бъдат унищожени сигурно, съгласно принципа за гарантиране подходящо ниво на сигурност, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“).

XII. Трансфер на данни

1.Всеки износ на данни от рамките на ЕС към страни извън ЕС (посочени в Регламента (ЕС) 2016/679 като „трети страни“) и Европейското икономическо пространство (ЕИП) (ЕС и Лихтенщайн, Норвегия и Исландия) са незаконни, освен ако има подходящо ниво на защита на основните права на субектите на данни. Прехвърлянето но лични данни извън ЕС е забранено, освен ако не се прилагат една или повече от указаните гаранции или изключения.

КРС не извършва трансфер на данни.

XIII. Регистър на дейностите по обработване по чл.30 от Регламента (ЕС) 2016/679

1. КРС е създала процес на инвентаризация на данните като част подход за справяне с рисковете и възможностите в процеса на спазване на политиката за съответствие с Регламента (ЕС) 2016/679. При инвентаризация на данните в КРС и в работния поток от данните се установяват:
    - Процесите, които използват лични данни;
    - Източниците на лични данни;
    - Броя на субектите на данни;
    - Описания на категориите лични данни и елементите във всяка категория;
    - Дейностите по обработване;
    - Целите на обработването, за което личните данни са предназначени;
    - Правното основание за обработването;
    - Получателите или категориите получатели на личните данни;
    - Основните системи и места за съхранение;
    - Сроковете за съхранение и заличаване.

2. КРС е наясно с рисковете, свързани с обработването на определени видове лични данни.

3. КРС оценява нивото на риска за лицата, свързани с обработването на личните им данни. Извършват се оценки на върху защитата на данните във връзка с обработването на лични данни от КРС и във връзка с обработването, предприето от други организации от името на КРС.

4. КРС прави ежегоден преглед на първоначално инвентаризираните данни, преразглежда вписаната информация в Регистъра по чл.30 в светлината на всякакви промени в дейностите на организацията и прави нужната актуализация на документирането.

XIV. Система за сигурност на информация

1. Понятия

В тази система „информационна сигурност“ се определя като:

1) Поверителност

Поверителност, означава да се гарантира, че информацията е достъпна само за онези, които имат разрешение за достъп до нея и следователно за предотвратяване както на преднамерен, така и случайно неоторизиран достъп до информацията на КРС и нейните системи (включително мрежи, интернет страница и други).

2) Цялостност

Това включва запазването на точността и пълнотата на информацията и методите за обработка и следователно изисква предотвратяване на преднамерено или случайно частично или пълно унищожаване или неразрешено изменение на материални активи или електронни данни.

3) Наличност

Това означава, че информацията и свързаните с нея активи трябва да бъдат достъпни за оправомощените потребители, когато са необходими и следователно физически сигурни. Компютърната мрежа трябва да е устойчива и КРС трябва да може да открива и да реагира бързо на инциденти (като вируси и други злонамерени програми), които застрашават постоянната наличност на активи, системи и информация. Трябва да има подходящи планове за непрекъснатост на работата.

4) Убеждение

Това означава, че ръководството, всички служители, стажанти, подизпълнители, консултанти по проекти и външни лица ще бъдат запознати с техните отговорности (които са определени в техните длъжностни характеристики или договори) за запазване на сигурността на информацията, да съобщава за нарушения на сигурността. Всички служители ще получат обучение за повишаване на информираността относно настоящата система за сигурност на информацията.

Активи на Комисията за регулиране на съобщенията

Активите на КРС са:

- Физически активи
- Информационни активи

- ***Физически активи***

Физическите активи на КРС са, включително, но не само компютърен хардуер, мрежово окабеляване за пренос на данни, телефонни системи, системи за архивиране и физически файлове с данни.

- ***Информационни активи***

Информационните активи включват информация, отпечатана или написана на хартия, предавана по общата или показана във филми или вербална в разговор, както и информация, съхранена по електронен път на сървъри, уебсайтове, персонални компютри, лаптопи, мобилни телефони и PDA устройства (персонален дигитален асистент) , както и на CD ROM (компактдиск, който е носител на информация за широка употреба) дискове, флопи дискове, USB памети, резервни касети и всякакви други цифрови или магнитни носители и информация, предавана по електронен път по всякакъв начин. В този контекст „данни“ включват и набор от инструкции, които указват на системата как да манипулират информацията (т.е. софтуера: операционни системи, приложения, помощни програми и т.н.) на КРС и такива партньори , които са част от интегрираната мрежа на КРС и са се присъединили към системата за сигурност.

Нарушение на сигурността

Нарушение на сигурността е всеки инцидент или дейност, която причинява или може да причини нарушение на наличността, поверителността или целостта на физическите или електронните информационни активи на Комисията за регулиране на съобщенията.

2. Предназначение на системата за сигурност на информация

Комисията за регулиране на съобщенията се ангажира да пази поверителността, целостта и наличността на всички физически и електронни информационни активи в цялата организация, за да запази конкурентно предимство, регулаторно и договорно съответствие и имидж.

Изискванията за защита на информацията ще продължат да бъдат съгласувани с целите на Комисията.

Системата за сигурност на информацията при изпълнение на целите и задачите си прилага действащата Политика за мрежова и информационна сигурност на Комисията за регулиране на съобщенията.

- Настоящата система е предназначена да осигури механизъм за обмен на информация, за електронни операции и за намаляване на свързаните с информация рискове да приемливи нива.
- Настоящата система осигурява идентифициране, оценка и контрол на свързаните с информацията рискове. Оценката на риска определя начина, по който се контролират рисковете, свързани с информацията. Допълнителни оценки на риска могат, когато е необходимо, да се извършат, за да се определят подходящи проверки за специфични рискове.

- Плановете за непрекъснатост на работата и плановете за действие при непредвидени обстоятелства, процедури за архивиране на данни, избягването на вируси и хакери, контрола на достъпа до системата и докладването на инциденти по сигурността на информацията са от основно значение за тази система.
- КРС има за цел да постигне конкретни, определени цели за информационна сигурност, които са разработени в съответствие с целите, контекста на организацията, резултатите от оценката на риска и плана за третиране на риска.
- Всички служители на КРС и определени в настоящата политика външни лица е необходимо да спазват тази политика. Всички служители са получили подходящо обучение.

Системата подлежи на непрекъснат, систематичен преглед и усъвършенстване. Тя ще бъде разглеждана, за да отговори на всякакви промени в оценката на риска или в плана за третиране на риска, поне веднъж годишно.