ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ
СОЦИАЛЕН ФОНД

ОПЕРАТИВНА ПРОГРАМА
ДОБРО УПРАВЛЕНИЕ

Проектът се осъществява с финансовата подкрепа на
Оперативна програма „Добро управление" 2014-2020г.
съфинансирана от Европейския социален фонд на
Европейския съюз- BG05SFOP001-3.015-0001-C01 –
„Повишаване на гражданското участие"

МЕХАНИЗЪМ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ ОСЪЩЕСТВЯВАНЕ НА ДЕЙНОСТТА

1. Обхват, предназначение и ползватели

Настоящият механизъм има за цел да създаде и приложи средства, осигуряващи спазването на законодателството в областта на защитата на личните данни, като това се отрази съществено върху процеса по оценка на въздействието върху защитата на данните (ОВВЗД) във всички отдели на фондация Социални норми в рамките на реализация на проект „Повишаване на гражданското участие"

2. Референтни Документи

Международно законодателство

Общ регламент относно защита на личните данни (Регламент (ЕС) 2016/679)

Директива за защита на личните данни в полицейската и наказателната дейност (Директива (ЕС) 2016/680)

Всеобща декларация за правата на човека

Конвенция за защита на правата на човека и основните свободи

Конвенция 108 за защита на лицата при автоматизираната обработка на лични данни

Харта на основните права на Европейския съюз

Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации

Рамково решение 2008/977/ПВР на Съвета относно защитата на личните данни, обработвани в рамките на полицейското и съдебно сътрудничество по

Проектът се осъществява с финансовата подкрепа на
Оперативна програма „Добро управление" 2014-2020г.
съфинансирана от Европейския социален фонд на
Европейския съюз- BG05SFOP001-3.015-0001-C01 –
„Повишаване на гражданското участие"

наказателноправни въпроси (валидно до влизане в сила на Директива (ЕС) 2016/680 за защита на личните данни в полицейската и наказателната дейност)

Директива (ЕС) 2016/681 за използването на резервационните данни на пътниците

Регламент (ЕС) 211/2011 на Европейския парламент и на Съвета относно гражданската инициатива

Регламент 611/2013 на Европейската комисия относно мерките, приложими за съобщаването на нарушения на сигурността на личните данни съгласно Директива 2002/58/ за правото на неприкосновеност на личния живот и електронните комуникации

Актове на ЕС по отношение на Шенген

Национално законодателство

Конституция на Република България

Закон за защита на личните данни

Закон за изменение и допълнение на Закона за защита на личните данни

Закон за електронните съобщения

Правилник за дейността на Комисията за защита на личните данни и нейната администрация

Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни - отменена, считано от 25.05.2018

Инструкция № 1 от 21 декември 2016 г. за обстоятелствата, при които предприятията, предоставящи обществени електронни съобщителни услуги, уведомяват потребителите за нарушения на сигурността на личните данни, формата и начина на уведомяването

3. Дефиниции

Общия регламент относно защита на данните на Европейския съюз дава коректна дефиниция на основните понятия и термини, които намират приложение в методологията:

„**Лични данни** - означава 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, културната или социална идентичност на това физическо лице.

Чувствителни лични данни -личните данни, които по своята същност са особено чувствителни по отношение на основните права и свободи, заслужават специфична защита, тъй като контекстът на тяхната обработка може да създаде значителни рискове за основните права и свободи. Тези лични данни включват лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикати, генетични данни, биометрични данни, с цел еднозначно идентифициране на физическо лице, данни относно здравето или данни, отнасящи се до пола на физическо лице, живот или сексуална ориентация

Оценката на въздействие на защита върху личните данни (ОВВЗД) - процес, предназначен да опише дейностите по обработка, да прецени необходимостта и пропорционалността на обработката, и да спомогне за управлението на рисковете за правата и свободите на физическите лица, произтичащи от обработката на лични данни.

Обработване - всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като

Проектът се осъществява с финансовата подкрепа на
Оперативна програма „Добро управление" 2014-2020г.
съфинансирана от Европейския социален фонд на
Европейския съюз BG05SFOP001-3.015-0001-C01 –
„Повишаване на гражданското участие"

събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване. „

4. Отговорности

Особената значимост на защитата на правата и свободите на лицата, както и тяхната неприкосновеност, както и тази на личен живот и поверителна информация, свързана с всеки един аспект от съществуването на субекта е водещ при създаване на международна и национална правна уредба, уреждаща надеждната и адекватна защита на личните данни на гражданите. Задължително е неговото инкорпориране във вътрешното законодателство на държавите членки, както и спазване на всички международни актове, по които България е страна в тази област. В Република България е създадена Комисия за защита на личните данни с решение на Народното събрание от 23 май 2002 година. Тя е независим държавен орган, който осъществява защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на Закона за защита на личните данни. Комисията е колегиален орган и се състои от четирима членове и председател, всички с четиригодишен мандат.

Съгласно Регламента и националното законодателство отговорността за обработката на личните данни пада върху всяко лице, което по някакъв начин обработва лични данни на лицата. То носи както отговорност за собствени действия свързани с обработката, но и за действията на трети лица, които в процеса на обработка могат да получат достъп до личните данни. Законът определя като надзорен орган Комисията за защита на личните данни и вменява задължение на администратора на лични данни да уведомява лицата изрично за това, какви лични данни събира, с каква цел за какъв срок, кое е отговорното лице по съхранение на данните, пред кой орган може да се обжалва действието на администратора,

Проектът се осъществява с финансовата подкрепа на
Оперативна програма „Добро управление" 2014-2020г.
съфинансирана от Европейския социален фонд на
Европейския съюз- BG05SFOP001-3.015-0001-C01 –
„Повишаване на гражданското участие"

предоставя ли се лична информация на лицата на трети страни, какви са правата има да бъдат забравени – т.е. да бъде заличени техните лични данни, право на корекция на личните им данни, право на информация и т.н.

Законът задължава администратора да определи лице, отговорно за защита на личните данни или длъжностното лице по защита на данните. Основната задача на длъжностното лице е да информира и съветва администратора и неговите служители по всички въпроси, свързани с обработването и защитата на личните данни. Длъжностното лице не определя целите и методите на съхранение на данните. То подпомага работата на администратора, но отговорността за цялостния процес е негова.

4.1. *Етап 1: Изброяване и групиране на дейности по обработване*

Отговорното лице за защита на личните данни да извърши цялостна ревизия на документите и процедурите свързани с приложение на GDPR в рамките на проекта, като това включва допълнително и всички дейности в номенкратурата на регистъра, да вземе под внимание всички нови дейности, които още не са включени в списъка, както и да изброи всички дейности по обработката на данни в регистъра свързани с нововъзникналите. Да се актуализират данните и ще се приведе документацията в изисквания от закона ред.

Служителят по защита на данните извършва преценка, кои дейности по обработка на данни ще бъдат оценявани заедно, ако има сходен рискна сходно или същото правно основание за възникване.

4.2. *Етап 2: Предварителен анализ*

Във всички случаи се извършва предварителен анализ на данните. Той е цялостен и всеобхватен и е свързан, както с оценка от гледна точка на актуалното законодателството, така и от гледна точка на целесъобразността, и ефективността на всяка дейност по обработка на данни.

Проектът се осъществява с финансовата подкрепа на
Оперативна програма „Добро управление" 2014-2020г.
съфинансирана от Европейския социален фонд на
Европейския съюз. BG05SFOP001-3.015-0001-C01 –
„Повишаване на гражданското участие"

Тази информация е базова в оценката на риска за личните данни на лицата от гледна точка на обработващия администратор.

4.3. *Етап 3: Определяне на необходимостта от пълна оценка на въздействието върху защитата на данните*

От важно значение за администратора на лични данни е да идентифицира дейностите по обработка на данни, да ги структурира и да ги анализира според нивото на риск, въз основа на данните от встъпителния въпросник. Ако на някой от въпросите от встъпителния въпросник бъде отговорено с "Да", трябва да се направи подробно обследване върху въздействието върху защитата на данните за тази конкретна дейност по обработка на данни.

Дори ако отговорите на всички въпроси от встъпителния въпросник са: "Не", служителят по защита на данните може да извърши обследване, ако компанията трябва да получи по-ясна представа за рисковете.

4.4. *Етап 4: Въпросник*

Създава се въпросник, който дава пълна информация за ревизираните дейности по обработката на данните, последователността на процесите, сроковете за действие във всеки етап, взетите мерки за опазване сигурността на информацията, факторите, които оказват влияние върху тях – като те се разделят на вътрешни и външни, възможните рискове и съответно степента на опасност от настъпване на рисково събитие и евентуалните последици от това.

4.5. *Етап 5: Идентифициране и регистриране на ключови рискове за сигурността*

Идентификацията и регистрирането на рисковете за сигурността на информацията се извършва на база на попълнения въпросник. Тази дейност дава възможност не само да бъде осигурена яснота по отношение на дейностите свързани с обработка

Проектът се осъществява с финансовата подкрепа на
Оперативна програма „Добро управление" 2014-2020г.
съфинансирана от Европейския социален фонд на
Европейския съюз BG05SFOP001-3.015-0001-C01 –
„Повишаване на гражданското участие"

на данните, но и да бъдат обективирани възможните рискове и съответно да се извърши оценка на риска на всяка дейност от случайно или незаконно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни. От своя страна регистриране на ключовите рискове ще доведе до създаване на система от превантивни мерки и ключове за защита на информацията. Дефинирайки нивото на риск за сигурността ще бъде възможно да се формулира и политиката при кризисни ситуации, при грешка и от особено значение при бедствия и аварии, когато е възможно да бъде повредена, унищожена или изгубена информацията.

4.6. *Етап 6: Мерки за намаляване на риска*

След като ключовите рискове бъдат идентифицирани и изброени, следва да се състави план за ефективно снижаване на риска в процеса на обработка на информация. В този план следва да се вземат мерки основно за превантивен контрол и съответно да се планират допълнителни защити/ втори ключ/ за защита на данните в съответните дейности. Необходимо е да бъдат предприети мерки за защита не само по отношение на съответните дейности, но те да въведат групирани по съответствие, като това се отнася и за системата в цялост. Програмата ще съдържа най-малко следната информация за дейностите, групите дейности и системата, превантивните мерки на всяко ниво, защитите и вторите ключове, отговорните лица и сроковете за изпълнение.

4.7. *Етап 7: Регистрация*

Всички въведени предпазни мерки се отразяват във въпросника.

5. Консултации с надзорния орган

Ако резултатите покажат, че дейността по обработка на данни би довела до висок риск, дори ако мерките за сигурност се прилагат, служителят по защита на данните

Проектът се осъществява с финансовата подкрепа на
Оперативна програма „Добро управление" 2014-2020г.
съфинансирана от Европейския социален фонд на
Европейския съюз- BG05SFOP001-3.015-0001-C01 –
„Повишаване на гражданското участие"

задължително планира и провежда срещи с надзорния орган, преди да се извърши обработката на данните.

На надзорният орган се предоставя цялата приложима информация, но не по-малко от:

- Цел и средства, за постигането на които ще бъдат използвани данните, обект на обработка
- Видовете данни, които ще се обработват
- Мерки за сигурност, предназначени за защита на данните
- Резултати от обследването

6. **Приложение 1** - Критерии за оценка

– Изготвен системен опис на обработването;
– Определени са целите и сроковете на обработването,определяне на данните, които са обект на обработка, както и получателите;
– Изготвени са и периодично са актуализирани регистрите на обработваните личните данни, и срока, за който ще се съхраняват личните данни;
– Дефиниране на вида хардуер, софтуер, интегрирани системи и мрежи за обработка на информация, други възможни канали и т. н.;
– Дефинирани са конкретна, изрично указана и легитимна цел или цели;
– Извършена е проверка за съответствие с приложимото законодателство, с етични норми и правила;
– Анализирани са данните и са ограничени до необходимото;
– Определен е срок за продължителност на съхранението;
– Лицата, чиито лични данни се обработват са информирани;
– Лицата, чиито лични данни се обработват са информирани за право на достъп и на преносимост на данните;

Проектът се осъществява с финансовата подкрепа на
Оперативна програма „Добро управление" 2014-2020г.
съфинансирана от Европейския социален фонд на
Европейския съюз BG05SFOP001-3.015-0001-C01 –
„Повишаване на гражданското участие"

- Лицата, чиито лични данни се обработват са информирани за право на коригиране и на изтриване;
- Лицата, чиито лични данни се обработват са информирани за право на възражение и на ограничаване на обработването;
- Лицата, чиито лични данни се обработват са информирани за начина на комуникация с обработващите лични данни;
- Взети са мерки при международно предаване на данни;
- Извършена е предварителна консултация с надзорния орган, когато това е необходимо;
- Взети са мерки за минимизиране на опасността от нарушение на правата и свободите на субектите на данни;
- Извършена е оценка на всеки риск от гледна точка на субектите на данни по произходът, естеството, спецификата и степента на рисковете, както и източниците на риска;
- Дефинирани са заплахите, които биха могли да доведат до нежелан достъп, изменения и загуба на данни;