ПРИМЕР !

РЪКОВОДСТВО

ЗА ОПРЕДЕЛЯНЕ НА ОБХВАТА НА СИСТЕМА ЗА УПРАВЛЕНИЕ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ (СУЗЛД)

1. ВЪВЕДЕНИЕ

Това Ръководство описва основните стъпки при определянето на обхвата на СУЗЛД, с цел създаването на предпоставки за постигане на съответствие с изискванията на **General Data Protection Regulation** - **GDPR** (по-специално с **чл.30** – "Регистри по дейностите на обработване на лични данни" и с **чл.32** - "Сигурност на обработките на лични данни") и Закон за защита на личните данни (ЗЗЛД).

Дейностите по определяне обхвата на СУЗЛД са от съществена важност за нейното изграждането, внедряването, поддръжне и развитие.

Точното и ясно дефиниране на границите на СУЗЛД, позволява да се избегне извършването на дейности, които не са необходими, а също и да се подобри качеството на анализа на риска към сигурността на личните данни, и съответния избор на контроли / защитни механизми.

СУЗЛД може да покрива цялата организация или част от нея, отделна система и/или услуга, в съответствие с местата и дейностите, които използват / работят с лични данни.

Целта е, СУЗЛД да покрива тези части от организацията, в които проблемите по сигурността на личните данни, могат да доведат до неприемливи последствия за бизнеса на организацията, като цяло, а също, да бъдат нарушени основни права и свободи на гражданите, субекти на лични данни (напр., правото на гражданите на защита на техните лични данни)

Това Ръководство се базира на:

- Описанията на бизнес процесите в организацията , вкл. продуктите / услугите, които ползват лични данни, експертната оценка за степентта на тяхната важност за бизнеса и потенциалното им влияние върху сигурността на личните данни;
- Описанията на информационните активи, осигуряващи изпълнението на бизнес процесите в организацията, ползващи лични данни;
- Изискванията за защита на личните данни, определени в националната регулаторна рамка – закони (ЗЗЛД), наредби, правилници и др. и на GDPR.

2. ОСНОВНИ СТЪПКИ

Основните стъпки за определяне обхвата на СУЗЛД са:

2.1. Стъпка №1 – Преглед и анализ на основните бизнес процеси в организацията, вкл., съответните продукти /услуги, които ползват лични данни и провеждане на експертната оценка за степентта на тяхната важност за бизнеса, и потенциалното им влияние върху сигурността на личните данни

Тази стъпка се извършва от **работна група,** включваща представители на всички звена в организацията, имащи отношение към изпълнението на съответните бизнес процеси, а също и експерти по информационна сигурност.

Забележка:
Описанието на съответните бизнес процеси (последователност на дейностите, обработки, изпълнители, входна и изходна информацияя / данни и др.) може да бъде налично в различни документи на организацията – Правилник за работата на организацията, Система за управление на качеството (политики, процедури, инструкции, форми за отчет), Система за управление на услугите и др., или да бъде представено от ръководители / експерти, които ръководят тяхното изпълнение.

Преди провеждането на анализ на основните бизнес процеси, ползващи лични данни се определя **организационния обхват** на СУЗЛД – организационни звена, адреси, в или извън страната, в ЕС или извън ЕС. Ако организацията има **Политика за изграждане, поддръжка и развитие на СУЗЛД**, то това е първоначалния, основен източник за определянето на организационния обхват.

Пример – описание на организационния обхват на СУЗЛД

№	Наименование на бизнес процеса, ползващ лични данни	Наименование на звенто / организацията, изпълняващо бизнес процеса	Местоположение на звеното / организацията, изпълняващо бизнес процеса
1	*Административно обслужване на персонала, клиентите и/или доставчиците*	Организацията – отдел „Административно обслужване“	София.....
2	*Финансово обслужване на персонала, клиентите и доставчиците*	Организацията – отдел „Административно обслужване“и **външен доставчик** (име) на услуги за финансово и счетоводно обслужване	София..... Пловдив.....
3	*Електронна търговия*	Организацията - отдел „Електронен магазин“ и **външен доставчик** (име) на услуги за финансово и счетоводно обслужване	София..... Пловдив.....
4	*Търговска дейност, пазарни проучвания и e-mail marketing*	Организацията -отдел „Търговия и маркетинг“ и **външен доставчик** (име) на услуги за ***e-mail marketing***	София .... САЩ, Бостон, ...

На база проведения преглед и анализ на бизнес процесите, ползващи лични данни, се изготвя **Опис (Регистър)** на бизнес процесите, личните данни, които използват и съответните обработки с тях.

Забележка:

*Ползваните в съответния бизнес процес лични данни, могат да бъдат класифицирани, като **общи** (напр., име, адрес, ЕГН, № лична карта, елктронна поща и др.), **чувствителни / специални** (раса, етнос, политически възгледи, религиозна или философска вяра, генетика, биометрия, здравно състояние, сексуален живот и сексуална ориентация) и **криминални** (свързани с нарушения, присъди и др.).*

*Видовете обработки на ползваните в бизнес процес лични данни включват всяка операция или съвкупност от операции, извършвана(и) чрез автоматични или чрез други средства (вкл. ръчно", като **събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждани или комбинирани, ограничавани, изтривани или унищожавани***

Пример:

№	Наименование на бизнес процеса, ползващ лични данни	Видове лични данни, ползвани в бизнес процеса	Видове обработки на личните данни, ползвани в бизнес процеса
1	*Административно обслужване на персонала, клиентите и/или доставчиците*	Общи лични данни: – име; – адрес; – електроинна поща;	– събиране; – записване; – структуриране; – съхранение; – унищожаване;
2	*Финансово обслужване на персонала, клиентите и/или доставчиците*	Общи лични данни: – име; – адрес; – ЕГН; – № лична карта; – телефон; – електронна поща;	– събиране; – записване; – структуриране; – употреба; – обмен; – съхранение; – унищожаване;
3	*Електронна търговия*	Общи лични данни: – име; – адрес; – електроинна поща; – данни за банкова карта;	– събиране; – записване; – структуриране; – употреба; – съхранение; – унищожаване;
4	*Търговска дейност, пазарни проучвания и e-mail marketing*	Общи лични данни: – име; – електроинна поща; – адрес; – телефон;	– събиране; – записване; – структуриране; – употреба; – обмен (трансфер); – извличане; – подреждане; – съхранение; – унищожаване;

Описанието на бизнес процесите е необходимо да се прегледа и анализира за да се създаде база за определяне, **на качествено ниво степентта на важност на всеки бизнес процес за**

постигане <u>бизнес целите на организацията</u>, и на степентта на потенциалното му влияние върху <u>сигурността на личните данни</u>.

Качественото определяне на **степентта** на важност на бизнес процесите и потенциалното им влияние върху сигурността на личните данни се могат да се дефинират, като: **несъществена, съществена, голяма и много голяма**

<u>Пример:</u>

№	Наименование на бизнес процеса, ползващ лични данни	Степен на важност на бизнес процеса за постигане на целите на организацията	Степен на потенциално влияние върху сигурността на личните данни
1	*Административно обслужване на персонала, клиентите и/или доставчиците*	съществена	голяма
2	*Финансово обслужване на персонала, клиентите и/или доставчиците*	голяма	много голяма
3	*Електронна търговия*	много голяма	много голяма
4	*Търговска дейност, пазарни проучвания и e-mail marketing*	голяма	съществена

<u>Забележки:</u>

*Бизнес процес „Финансово обслужване на персонала, клиентите и/или доставчиците“ се извършва по договор, с **външна** организация, базирана в страната.*

*Бизнес процес „Търговска дейност, пазарни проучвания и e-mail marketing” се извършва от организацията, с изключение на дейностите, свързани с **e-mail marketing**, които в преобладаващата си част се изпълняват по договор с **външна** организация, базирана в страна **извън ЕС**.*

2.2. Стъпка №2 – “Количествена оценка на бизнес процесите”

Вход за тази стъпка са резултатите от изпълнението на стъпка 1 “Преглед и анализ на основните бизнес процеси в организацията...”

Оценката на бизнес процесите се извършва, отчитайки определените на **качествено ниво** степени на важност и потенциал на влияние на бизнес процеса (напр. несъществена, съществена, голяма, много голяма) и техните последващи остойностявания, по предварително приети количествени коефициенти на съответствие.

<u>Пример:</u> Остойностяване за „степен на важност на бизнес процеса“

Таблица на съответствието – “качествена оценка – количествен коефициент” за **степен на важност** на бизнес процеси

№	Степен на важност на бизнес процеса за постигане на целите на организацията (качествена оценка)	Степен на важност на бизнес процеса за постигане на целите на организацията (количествен коефициент)
1	несъществена	0.1
2	съществена	0.4

3	голяма	0.7
5	много голяма	1.0

<u>Пример:</u> Остойностяване за „степен на потенциално влияние към сигурността на личните данни“.

Таблица на съответствието – “**качествена оценка – количествен коефициент**” за **степен на потенциално влияние на бизнес процес върху сигурността на личните данни**

№	**Степен на потенциално влияние върху сигурността на личните данни (качествена оценка)**	**Степен на потенциално влияние върху сигурността на личните данни (количествен коефициент)**
1	несъществена	0.2
2	съществена	0.5
3	голяма	0.8
5	много голяма	1.0

<u>Пример:</u> Интегрирана оценка на бизнес процес – важност за бизнеса и за влияние върху сигурността на личните данни

<u>Забележка:</u>
Интегрираната оценка *се получава след* ***събиране*** *на съответните количествени коефициенти за важност и влияние.*

№	**Наименование на бизнес процеса, ползващ лични данни**	**Степен на важност на бизнес процеса за постигане на целите на организацията**	**Степен на потенциално влияние върху сигурността на личните данни**	**Интегрирана оценка на бизнес процес**
1	*Административно обслужване на персонала, клиентите и/или доставчиците*	съществена / 0.4	голяма / 0.8	**1.2**
2	*Финансово обслужване на персонала, клиентите и/или доставчиците*	голяма / 0.7	много голяма / 1.0	**1.7**
3	*Електронна търговия*	много голяма / 1.0	много голяма / 1.0	**2**
4	*Търговска дейност, пазарни проучвания и e-mail marketing*	голяма / 0.7	съществена / 0.5	**1.2**

<u>Забележка:</u>
Колкото е ***по-голяма по стойност интегрираната оценка*** *на даден бизнес процес,* ***толкова е и по-голяма неговата важност, както за бизнеса, така и за сигурността на личните данни****, които обработва.*

След завършването на работата по тази стъпка организацията ще разполага с:
- организационния обхват на СУЗЛД;

- бизнес обхвата на СУЗЛД и съответните качествени, количествени, и интегрирани оценки на бизнес процесите, ползващи лични данни (по отношение на тяхната важност за бизнеса и потенциалното им влияние върху сигурността на личните данни, които ползват).

2.3. Стъпка №3 – "Определяне на информационните активи, осигуряващи изпълнението на съответните бизнес процеси, ползващи лични данни"

Вход за тази стъпка са идентифицираните бизнес процеси, техните качествени, количествени и интегрирани оценки по отношение приноса им към бизнеса, и потенциалното им влияние към сигурността на личните данни. (изход от изпълнението на стъпка 2)

Тази стъпка се обикновено се извършва от **работна група,** включваща представители на всички звена в организацията, имащи отношение към изпълнението на съответните бизнес процеси, а също и експерти по информационна сигурност.

За **всеки бизнес процес, ползващ лични данни** се описват информационните активите, осигуряващи неговото изпълнение в обхват (съгласно Политиката за изграждане, поддръжка и развитие на СУЗЛД):

- **хардуер** - компютри, сървери, средства за съхраняване, периферна техника, мрежово оборудване, комуникационна инфраструктура (вкл.мрежово окабеляване), гарантирано електрозахранване, климатизация и др., както е приложимо;
- **софтуер** - системи за управление на бази данни съдържащи лични данни; приложения и системи за обработка на лични данни; софтуерен инструментариум за системен и/или софтуерен инженеринг; приложения за клиенти; софтуер за тестване и др., както е приложимо;
- **документи, съдържащи лични данни** – всякакъв тип документи в електронен вид и разпечатани на хартия;
- **персонал** - наетите служители (постоянно и временно наети, собствени и външни) одитори (вътрешни и външни), доставчици на услуги, представители на заинтересованите и свързани лица, страни по договори, консултанти, посетители или представители на други организации, имащи отношение при изпълнението на съответния бизнес процес и достъп до активи, работещи с лични данни на организацията и др., както е приложимо.

Пример: - *Информационни активи, осигуряващи изпълнението на бизнес процес "**Електронна търговия**"*

Идент. № на актива	Описание на актива	Функция на актива	Организационна единица, собственик на актива	Персонален собственик на актива (длъжност / име)	Достъп до актива (длъжност / име / организация)
	ХАРДУЕР				
00001H	Компютър	Събиране, записване, съхранение, обмен и унищожаване на лични данни	Отдел "Електронен магазин""	.....	.....
00002H	Сървер.за.....	Записване, съхранение , обмен и унищожаване	Отдел "ИТ""	.....	.....

		на лични данни			
	СОФТУЕР				
00001S	Приложение „Регистър клиенти“	Събиране, записване, структуриране, съхранение, обмен и унищожаване на лични данни	Отдел “Електронен магазин“”	.....	.....
00002S	Приложение за анализ на клиентите и покупките	Събиране, записване, структуриране, извличане, съхранение, обмен и унищожаване на лични данни	Отдел “Електронен магазин“”	.....	.....
00003S	Приложение за финасово и счетоводно обслужване на покупките / клиентите	Записване, структуриране, извличане, съхранение, обмен и унищожаване на лични данни	Отдел “Електронен магазин“ и **външна** организация	.....	.....
	Документи, съдържащи лични данни				
00001D	Обобщена, месечна справка на клиентите по типове покупки (в електронене и разпечатан вид)	Осигурява информация на Ръководството на Организацията за анализи и вземане на решения по продажбите	Отдел “Електронен магазин“		
00002D	Ежедневна справка за клиентите, направили покупки	Осигурява информация на външна организацията, извършваща финансово – счетоводни услуги	Отдел “Електронен магазин“ и **външна** организация		
.....	.....	.....	.....		

Забележки:
Персонала, работещ и/или имащ достъп до лични данни не е определен, като актив в отделни редове на горната таблица, тъй-като тази информация се съдържа в последните две колони от нея.
***Персонален собственик** на актив е физическото лице, което работи с този актив и има отговорности, свързани с неговата защита.*
*В допълнение към направеното по-горе описание, **може да се добави вида на личните данни**, с които работят съответните активи (напр., към втората колона на горната таблица).*

След завършването на изпълненията на тази стъпка, организацията разполага с **Опис на активите**, осигуряващи изпълнението на бизнес прицесите, ползващи лични данни.

Важността на активите за бизнеса и тяхното потенциално влияние върху сигурността на личните данни, **съответствуват** на качествените, количествени и интегрирани оценки, определени за съответния бизнес процес. В този смисъл, **всички активи** (хардуер, софтуер, документи и персонал), разгледани като пример по-горе (за бизнес процес „Електронна търговия“) ще имат: **степен на важност за бизнеса „много голяма“ и потенциално влияние към сигурността на личните данни „много голя“.**

По същия начин могат да се определят активите в останалите бизнес процеси от обхвата на СУЗЛД, и на тях да присвоят съответните степени за важност и влияние.

Определянето на тези степени (количествени и кчествени) за активите, **се използва при определянето на нивата на риск към тях**. Например, колкото е по-голяма интегрираната оценка за даден актив, толкова по-голямо ще бъдат неблагоприятните последствия при пробив на неговата сигурност - за бизнеса и личните данни, а това повишава и съответното ниво на риск, и насочва какви адекватни контролни / защитни механизми дасе изберат и приложат.

2.4. Стъпка №4 – “Документиране на установения обхват на СУЗЛД”

На тази стъпка се подготвя окончателен документ “**Обхват на СУЗЛД**” и се представя на Ръководството на организацията за съгласуване и одобряване, след което той става основание за извършване на последващите дейности по изграждането на системата – **анализ и оценка на риска към активите, избор на контроли (механизми за защити) за тях и др**.

<u>Забележка:</u>

Този документ се променя при планирани и/или фактически настъпили изменения в бизнес процесите, активите и персонала, който осигурява тяхното изпълнение, като всички стъпки от процеса или част от тях се изпълняват, в съответствие с обхвата и детайлите на измененията.

Крайния документ включва:

Списъци на **бизнес процесите**, ползващи лични данни и на **информационните активи,** осигуряващи тяхното изпълнение:

- Хардуер;
- Софтуер;
- Документи, съдържащи лични данни;
- Персонал

Така опраделения <u>обхват на СУЗЛД</u> е основа за провеждането на анализ и оценка на рисковете към сигурността на личните данни, и за последващото определянето на конкретни контролни / защитни механизми и/или средства за тяхната защита.

Обхвата на СУЗЛД е база заизпълнението на изискванията и постигане на съответствие с GDPR, по-специално с **чл.30** – “Регистри по дейносттите на обработване на лични данни“ и с **чл.32** - “Сигурност на обработките на лични данни“.