					Въведете тук наименованието на регистрираното юридическо лице							
Номер на документа: PII19					Заглавие на документа: **Политика за поверителност на служителите**							
Версия: 1.0		Дата на влизане в сила: 01.01.2025			Собственик на документа:							
X	Политика		Стандарт		Процедура		Формуляр		Регистър		Друго	

История на редакциите				
Номер на редакцията	**Дата на редакцията**	**Промени**	**Прегледано от**	**Собственик на процеса**

Одобрения			
Име	**Длъжност**	**Дата**	**Подпис**

Съгласуване със стандарти и регулации

Стандарт / регулация	Клауза / контрол / член	Приложимост	Вид покритие	Коментар
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Доказателства за поверителност на служителите и оперативен контрол
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Мониторинг, несъответствия и коригиращи действия
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Цели на ЧР, връзка с правното основание, критерий за задействане на DPIA, съвместна отговорност и записи
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Both	Supporting	Договори с обработващи лични данни в областта на ЧР, нареждания, съдействие и записи
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Supporting	Задължения, права и маршрутизиране при автоматизирано вземане на решения за служители
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Събиране, обработване, минимизиране и връзка със сроковете за съхранение
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Both	Supporting	Записи за разкриване и обработване на правно обвързващо разкриване
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Защита на ЧР записи и доказателства от журнализиране

GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Принципи за поверителност на служителите и отчетност
GDPR	Article 6; Article 9; Article 10	Controller	Supporting	Законосъобразност, специални категории данни и данни от проверки на миналото
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Прозрачност и уведомления към служителите
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Supporting	Права на служителите и маршрутизиране при автоматизирано вземане на решения
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Управление, съвместни администратори, обработващи лични данни, записи, сигурност, DPIA и консултиране
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Цел, събиране, минимизиране, използване, съхранение и разкриване
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Прозрачност, участие, отчетност, сигурност и съответствие
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Controller	Supporting	Цел на PII, събиране, минимизиране, съхранение и участие на субекта на данни
ISO/IEC 29151:2022	Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2	Controller	Supporting	Контроли през жизнения цикъл на работната сила за защита на PII

ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3	Both	Supporting	Оценяване, мониторинг и контрол на промените при обработващи лични данни в областта на ЧР
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Връзка с риска за поверителността в ЧР и критериите за задействане на DPIA
ISO/IEC 27002:2022	Controls 5.34; 6.1; 6.2; 6.5; 6.6	Both	Supporting	Защита на PII и жизнен цикъл на информационната сигурност на работната сила
ISO/IEC 27002:2022	Controls 8.15; 8.16	Both	Supporting	Дейности по журнализиране и мониторинг

1. Обхват

1.1 Тази политика определя изискванията за поверителност на служителите при събиране, използване, разкриване, връзка със сроковете за съхранение, уведомяване, обработване на права, наблюдение на служители, поддръжка от обработващи лични данни и управление на доказателства за лични данни на служители в рамките на системата за управление на неприкосновеността на личната информация.

1.2 За целите на тази политика „лични данни на служители“ включва PII, свързана със служители, кандидати за работа, бивши служители, изпълнители, временен персонал, стажанти, командировани лица и други участници в работната сила, когато организацията обработва тяхната PII за цели, свързани с работната сила, подбор, заетост, ангажимент, възнаграждения, придобивки, сигурност, съответствие, администриране на работното място или свързани бизнес цели.

1.3 Тази политика се прилага в контексти на администратор и съвместен администратор, когато организацията определя целите и средствата за обработване на лични данни на служители.

1.4 Тази политика се прилага и в контексти на обработващ лични данни и подизпълнител по обработване, когато организацията обработва лични данни на служители от името на клиент, предходен обработващ лични данни или друг администратор съгласно документирани нареждания.

1.5 Тази политика обхваща следните въпроси:

1.5.1 събиране на данни за служители;

1.5.2 цели на обработването от ЧР;

1.5.3 уведомления за поверителност към служителите;

1.5.4 обработване на права на служителите;

1.5.5 връзка със сроковете за съхранение;

1.5.6 наблюдение на служители;

1.5.7 вътрешно разкриване;

1.5.8 контроли за обработващи лични данни в областта на ЧР, заплати, HRIS, придобивки, проверки на миналото и външно възложени ЧР услуги, когато е приложимо;

1.5.9 инциденти с лични данни на служители, несъответствия, коригиращи действия и доказателства за подобрение.

1.6 Тази политика не създава отделен регистър за поверителност в ЧР, регистър за поверителност на служителите, регистър на обработването от ЧР, регистър за наблюдение на служители, регистър за проверки на миналото, регистър на ЧР доставчици, регистър на правата на служителите или регистър на инциденти със служители.

1.7 Доказателствата за обработване на служители се записват в REG02, REG04, REG06, REG07, REG08, REG10 и REG12.

1.8 Тази политика не предоставя съвети по трудово право, съвети във връзка с трудови отношения, правни коментари относно работнически съвети, съдържание за дисциплинарни процедури, съдържание за оперативни процедури по заплати или специфични за юрисдикция шаблони за трудови документи.

1.9 Тази политика не дублира следните въпроси:

1.9.1 управление на PIMS в PII01;

1.9.2 отчетност по роли в PII02;

1.9.3 инвентар на обработването и собственост върху правното основание в PII03;

1.9.4 управление на съдържанието на уведомленията за поверителност в PII04;

1.9.5 функциониране на съгласието и предпочитанията в PII05;

1.9.6 работен поток за права на субекта на данни в PII06;

1.9.7 методология за риска за поверителността и DPIA в PII07;

1.9.8 контролни точки за privacy-by-design в PII08;

1.9.9 базови правила за събиране, използване, разкриване и споделяне в PII09;

1.9.10 изпълнение на съхранение, изтриване и унищожаване в PII10;

1.9.11 управление на точността и качеството в PII11;

1.9.12 управление на жизнения цикъл на обработващи лични данни, подизпълнители по обработване и трети страни в PII12;

1.9.13 контроли за механизми за международно прехвърляне в PII13;

1.9.14 внедряване на сигурност и контрол на достъпа в PII14;

1.9.15 обработване на инциденти и нарушения в PII15;

1.9.16 управление на обучение и осведоменост в PII16;

1.9.17 контрол на документирана информация в PII17;

1.9.18 управление на мониторинга, одита и подобрението на PIMS в PII18;

1.9.19 контроли за AI и автоматизирано вземане на решения в PII21, когато тази незадължителна политика е включена.

2. Цел

2.1 Целта на тази политика е да гарантира, че лични данни на служители се обработват само за документирани, одобрени, прозрачни, пропорционални и отчетни цели, свързани с работната сила, и че доказателствата за поверителността на служителите се поддържат в каноничните регистри на PIMS, без да се създава отделен слой доказателства за поверителност в ЧР.

2.2 Тази политика подпомага последователното обработване на дейностите със служителски данни чрез свързване на дейностите по обработване на служители с REG02, уведомленията за поверителност към служителите с REG07, исканията за упражняване на права на служители с REG06, риска за поверителността в ЧР и критериите за задействане на DPIA с REG04, обработващите лични данни в областта на ЧР и доставчиците на заплати или HRIS с REG08, инцидентите с лични данни на служители с REG10, както и изключенията, несъответствията, коригиращите действия и доказателствата от мониторинг с REG12.

3. Цели

3.1 Целите на тази политика са да:

3.1.1 поддържа доказателства за инвентара на обработването на служители в REG02;

3.1.2 документира източниците за събиране на данни за служители, категориите PII, целите, системите, получателите и връзката със сроковете за съхранение;

3.1.3 поддържа доказателства за уведомленията за поверителност към служителите в REG07;

3.1.4 маршрутизира риска за поверителността на служителите и критериите за задействане на DPIA чрез REG04;

3.1.5 маршрутизира исканията за упражняване на права на служителите чрез REG06;

3.1.6 поддържа доказателства за обработващи лични данни в областта на ЧР, заплати, HRIS, придобивки, проверки на миналото и външно възложени ЧР услуги в REG08;

3.1.7 гарантира, че наблюдението на служители е документирано, пропорционално, преглеждано и ескалирано чрез REG04 и REG12, когато е приложимо;

3.1.8 маршрутизира предполагаеми инциденти с лични данни на служители чрез REG10;

3.1.9 записва изключения, несъответствия, коригиращи действия и действия за подобрение, свързани с поверителността на служителите, в REG12;

3.1.10 избягва съвети по трудово право и правни коментари относно работнически съвети в оперативните клаузи;

3.1.11 избягва дублиращи регистри, роли, формуляри, информационни табла или специфични за ЧР доказателствени обекти.

4. Изявления на политиката

4.1 Инвентар на обработването на служители и цели на обработването от ЧР

4.1.1 [Controller] Process Owner / Business Owner MUST запише всяка дейност по обработване на служители в REG02, преди лични данни на служители да бъдат събрани, генерирани, импортирани, използвани или разкрити.

4.1.2 [Controller] Process Owner / Business Owner MUST документира категориите лични данни на служители, групата служители, източника на събиране, целта на обработването, системата, категорията вътрешни получатели, категорията външни получатели и връзката със сроковете за съхранение в REG02, преди дейността по обработване да бъде одобрена.

4.1.3 [Controller] Privacy Lead / PIMS Manager MUST прегледа всяка нова или съществено променена дейност по обработване на служители в REG02, преди дейността по обработване да бъде одобрена за експлоатация.

4.1.4 [Conditional] Data Protection Officer / Privacy Advisor MUST запише съвет относно поверителността в REG04 преди одобряване на обработване на служители, включващо специални категории PII, данни за присъди и нарушения, проверка на миналото, данни за трудово здраве, биометрични данни, данни за местоположение, наблюдение на служители или обработване, което може съществено да засегне служител.

4.1.5 [Processor] Privacy Lead / PIMS Manager MUST запише нареждането на клиента, целта на услугата, категориите лични данни на служители на клиента и връзката с роля на обработващ лични данни в REG08, преди да обработва лични данни на служители на клиента като външно възложена услуга за ЧР, заплати, придобивки, HRIS, проверки или поддръжка на работната сила.

4.1.6 [Joint Controller] Privacy Lead / PIMS Manager MUST запише разпределението на отговорностите между съвместните администратори за обработване на лични данни на служители в REG08, преди съвместната дейност по обработване на служители да започне.

4.2 Събиране на данни за служители и уведомления за поверителност към служителите

4.2.1 [Controller] Process Owner / Business Owner MUST ограничи събирането на лични данни на служители до категориите, документирани в REG02, преди да започне събиране при подбор, въвеждане в длъжност, администриране на заетостта, администриране на придобивки, обработване на заплати, проверки, наблюдение или освобождаване.

4.2.2 [Controller] Process Owner / Business Owner MUST запише източника на лични данни на служители, събрани от трети страни, в REG02, преди източникът за събиране от трета страна да бъде използван.

4.2.3 [Controller] Privacy Lead / PIMS Manager MUST поддържа запис за уведомление за поверителност към служителите в REG07, преди лични данни на служители да бъдат събрани пряко или непряко за нова или съществено променена цел.

4.2.4 [Controller] Process Owner / Business Owner MUST потвърди, че текущото уведомление за поверителност към служителите, записано в REG07, е налично преди събиране при подбор, събиране при въвеждане в длъжност, активиране на наблюдение, записване за придобивки, проверка на миналото или съществена промяна в обработването на служители.

4.2.5 [Conditional] Data Protection Officer / Privacy Advisor MUST прегледа записа за уведомление за поверителност към служителите в REG07 преди публикуване, когато уведомлението обхваща наблюдение на служители, проверка на миналото, специални категории PII, данни за присъди и нарушения, автоматизирано вземане на решения или съществено променена цел за обработване на служители.

4.2.6 [Processor] Vendor / Procurement Owner MUST запише отговорностите за канала за събиране, насочен към служителите, в REG08, преди управлявана от обработващ лични данни услуга за ЧР, заплати, HRIS, придобивки, проверки или външно възложена ЧР услуга да събира лични данни на служители от името на клиент.

[... Раздели 4.3–8 не са включени в тази предварителна версия. Закупете пълния документ за достъп до пълното съдържание. ...]

9. Изключения

9.1.1 [All] Process Owner / Business Owner MUST запише искане за изключение в REG12, преди да се отклони от което и да е изискване на тази политика.

9.1.2 [Conditional] Data Protection Officer / Privacy Advisor MUST запише съвет в REG12 преди одобряване на изключение, засягащо наблюдение на служители, обработване на права на служители, проверка на миналото, специални категории PII, данни за присъди и нарушения или обработване на служители с високо въздействие.

9.1.3 [Conditional] Top Management MUST одобри изключения, свързани с поверителността на служителите, в REG12 преди активиране, когато изключението засяга високорисково обработване на служители, наблюдение на служители, външно разкриване, зависимост от обработващ лични данни или нерешено коригиращо действие.

9.1.4 [All] Privacy Lead / PIMS Manager MUST зададе дата на изтичане, която не надвишава 90 дни, за всяко изключение, свързано с поверителността на служителите, в REG12, преди изключението да бъде активирано.

9.1.5 [All] Privacy Lead / PIMS Manager MUST прегледа всяко изключение, свързано с поверителността на служителите, в REG12 в рамките на пет работни дни преди изтичане.

9.1.6 [All] Privacy Lead / PIMS Manager MUST закрие или ескалира всяко изтекло изключение, свързано с поверителността на служителите, в REG12 в рамките на пет работни дни след изтичане.

10. Прилагане на политиката

10.1.1 [All] Privacy Lead / PIMS Manager MUST запише несъответствие в REG12 в рамките на пет работни дни, когато при обработването на лични данни на служители липсват изискваните доказателства в REG02, REG07, REG08, REG04 или REG06.

10.1.2 [Conditional] Incident Response Coordinator MUST запише предполагаем неоторизиран достъп до лични данни на служители, разкриване, загуба или компрометиране в REG10 в рамките на един работен ден от установяването.

10.1.3 [Controller] Privacy Lead / PIMS Manager MUST предотврати одобряването на ново наблюдение на служители в REG12, когато липсват изискваните доказателства в REG02, REG04 или REG07.

10.1.4 [Both] Vendor / Procurement Owner MUST спре ново разкриване на лични данни на служители към ЧР доставчик в REG08, когато липсват изискваните доказателства за обработващ лични данни, подизпълнител по обработване, нареждане или съдействие.

10.1.5 [All] Top Management MUST прегледа повтарящи се несъответствия, свързани с поверителността на служителите, в REG12, когато една и съща категория възникне два или повече пъти в рамките на подвижен 12-месечен период.

10.1.6 [All] Internal Audit / Compliance Reviewer MUST провери доказателствата за закриване в REG12, преди да закрие одитни констатации, включващи обработване на лични данни на служители, уведомления към служители, наблюдение на служители, права на служители или ЧР доставчици.

11. Преглед и поддръжка

11.1.1 [All] Privacy Lead / PIMS Manager MUST преглежда тази политика в REG12 поне веднъж годишно.

11.1.2 [Conditional] Privacy Lead / PIMS Manager MUST прегледа тази политика в REG12 в рамките на 30 дни от съществена промяна в обработването на служители, наблюдението на служители, ЧР системите, договореностите за заплати, доставчиците на HRIS, доставчиците на придобивки, доставчиците за проверки на миналото или външно възложените ЧР услуги.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUST прегледа предложените съществени промени в тази политика в REG12 преди одобрение от Top Management.

11.1.4 [All] Top Management MUST одобри съществени промени в тази политика в REG12 преди публикуване.

11.1.5 [All] Privacy Lead / PIMS Manager MUST актуализира REG02, REG07 или REG08 в рамките на 15 работни дни след като одобрена промяна в политиката засегне записи за обработване на служители, уведомления за поверителност към служителите или доказателства за ЧР доставчици.

11.1.6 [All] Internal Audit / Compliance Reviewer MUST записва наблюдения за ефективността на прегледа на тази политика в REG12 по време на планирания цикъл на вътрешен одит на PIMS.

12. Свързани политики

12.1 Тази политика се подкрепя от следните свързани политики:

12.2 PII01 - Политика за система за управление на неприкосновеността на личната информация

12.3 PII02 - Политика за роли, отговорности и отчетност във връзка с поверителността

12.4 PII03 - Политика за инвентар на обработването на PII и правно основание

12.5 PII04 - Политика за уведомления за поверителност и прозрачност

12.6 PII05 - Политика за управление на съгласие и предпочитания

12.7 PII06 - Политика за управление на права на субекта на данни относно PII

12.8 PII07 - Политика за оценка на риска за поверителността и DPIA

12.9 PII08 - Политика за поверителност още при проектиране и по подразбиране

12.10 PII09 - Политика за събиране, използване, разкриване и споделяне на PII

12.11 PII10 - Политика за съхранение, изтриване и унищожаване на PII

12.12 PII11 - Политика за точност и качество на PII

12.13 PII12 - Политика за управление на поверителността при обработващи лични данни, подизпълнители по обработване и трети страни

12.14 PII13 - Политика за международно прехвърляне на PII

12.15 PII14 - Политика за сигурност и контрол на достъпа до PII

12.16 PII15 - Политика за управление на инциденти и нарушения, свързани с PII

12.17 PII16 - Политика за обучение, осведоменост и компетентност относно поверителността

12.18 PII17 - Политика за документирана информация и управление на доказателства в PIMS

12.19 PII18 - Политика за мониторинг, одит и подобрение на PIMS

12.20 PII21 - Политика за поверителност при AI и автоматизирано вземане на решения, когато е включена в обхвата на незадължителното допълнително издание

13. Референтни стандарти и рамки

13.1 Тази политика е картографирана към следните стандарти и регулации. Картографирането обяснява как политиката подпомага посочените изисквания и идентифицира вътрешните клаузи, които ги прилагат или подкрепят.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Картографирано към документирани доказателства за поверителността на служителите, оперативни контролни точки за одобрение, записи за обработващи лични данни в областта на ЧР, уведомления към служители, записи за наблюдение, обработване на изключения и доказателства за внедряване. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.3; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.1; 7.1.3].

13.2.2 **Clause 9.1; Clause 10.2** - Картографирано към мониторинг на поверителността на служителите, показатели, одитни доказателства, извадкова проверка на наблюдението на служители, обработване на несъответствия, коригиращо действие и подобрение. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 4.6.7; 8.1.1; 8.1.4; 8.1.7; 10.1.1; 10.1.5].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Картографирано към цели на обработване на служители, връзка с правното основание, маршрутизиране на риска за поверителността и DPIA, разпределение между съвместни администратори и записи за обработване в REG02 и REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.6; 4.2.2; 4.6.1; 4.6.2].

13.2.4 **Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Картографирано към договори с обработващи лични данни в областта на ЧР, документирани нареждания, обработване на лични данни на служители на клиента, съдействие от обработващ лични данни и записи за обработващи лични данни в REG08. Addressed by clauses [4.1.5; 4.2.6; 4.4.4; 4.5.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11** - Картографирано към обработване на права на служителите, съвети при комплексни права и маршрутизиране на автоматизирани решения или обработване с високо въздействие чрез REG06 и REG04. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9** - Картографирано към ограничаване на събирането на данни за служители, одобрено вътрешно използване, минимизиране, връзка със сроковете за съхранение и маршрутизиране на изключения за съхранение. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.6.1].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Картографирано към външни разкривания на лични данни на служители, записи за

споделяне на данни, разрешение за разкриване от обработващ лични данни и маршрутизиране на инциденти, свързани с разкриване. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.7.6].

13.2.8 **Annex A.3.14; Annex A.3.25** - Картографирано към защита на записи за поверителност на служителите, доказателства от журнали за наблюдение на служители и предполагаема злоупотреба или компрометиране на данни от наблюдение на служители. Addressed by clauses [4.6.4; 4.6.6; 4.6.7; 7.1.2].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Картографирано към законосъобразно, добросъвестно, прозрачно, ограничено до целите, минимизирано, свързано със срокове за съхранение и отчетно обработване на лични данни на служители. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.1; 4.3.3; 4.4.1; 4.4.5].

13.3.2 **Article 6; Article 9; Article 10** - Картографирано към връзка с правното основание, маршрутизиране на специални категории лични данни на служители, маршрутизиране на чувствителна PII, свързана с трудово здраве и заетост, както и маршрутизиране на данни за присъди и нарушения или проверки на миналото. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.2.2; 4.7.3].

13.3.3 **Article 12; Article 13; Article 14** - Картографирано към прозрачност за служителите, записи за уведомления за поверителност към служителите, критерии за уведомяване при пряко и непряко събиране и доказателства за уведомления при наблюдение. Addressed by clauses [4.2.3; 4.2.4; 4.2.5; 4.6.5].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21; Article 22** - Картографирано към маршрутизиране на права на служителите, доказателства за искания, съвети при комплексни искания и маршрутизиране при автоматизирани решения. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Картографирано към управление от администратора, разпределение между съвместни администратори, управление на обработващи лични данни в областта на ЧР, записи за обработване, сигурно обработване, маршрутизиране към DPIA и участие на консултант по поверителността. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.6.2; 4.6.3; 4.6.6; 4.7.1; 4.7.6].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Картографирано към определяне на целите за служителите, ограничаване на събирането, минимизиране, ограничаване на използването, ограничаване на съхранението и ограничаване на разкриването. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.6.1].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Картографирано към прозрачност, участие на служителите, поддръжка на правата на служителите, отчетност, информационна сигурност и доказателства за съответствие с поверителността. Addressed by clauses [4.2.3; 4.2.4; 4.5.1; 4.5.2; 4.5.5; 4.6.4; 4.6.6; 4.6.7; 4.7.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Картографирано към записи за цели на PII, контроли за събиране, минимизиране, връзка със сроковете за съхранение, ограничаване на разкриването и участие или поддръжка на достъп за служителите. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.4; 4.4.1; 4.4.2; 4.5.1; 4.5.4].

13.5.2 **Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2** - Картографирано към контроли от жизнения цикъл на работната сила за защита на PII, релевантни за проверки, условия, връзка с прилагането при нарушения на поверителността и преглед на съхранението при прекратяване или промяна на заетостта. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.5; 10.1.1; 10.1.5].

13.5.3 **Clause 15.1.2; Clause 15.2.2; Clause 15.2.3** - Картографирано към оценяване на обработващи лични данни в областта на ЧР, мониторинг на обработващи лични данни в областта на ЧР, преглед на ЧР доставчици и доказателства за промяна на услугата в REG08. Addressed by clauses [4.4.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6].

13.6 ISO/IEC 29134:2020

13.6.1 **Clause 5.1; Clause 6.2** - Картографирано към ползите от оценката на въздействието върху поверителността и определянето на риск за поверителността в ЧР или критерий за задействане на DPIA за наблюдение на служители и ЧР обработване с високо въздействие, без да се дублира методът за DPIA. Addressed by clauses [4.1.4; 4.3.3; 4.6.2; 4.6.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 6.1; 6.2; 6.5; 6.6 - Картографирано към защита на PII, проверки, условия за работната сила, отговорности след промяна на заетостта и очаквания за поверителност като контроли от жизнения цикъл на работната сила, подкрепящи PII. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.4; 4.7.2; 4.7.3].

13.7.2 Controls 8.15; 8.16 - Картографирано към журнали за наблюдение на служители, дейности по мониторинг, ограничаване на целта на журналите и преглед на доказателства от наблюдение. Addressed by clauses [4.6.1; 4.6.2; 4.6.4; 4.6.6; 4.6.7].