**ПОЛИТИКА ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ**
(цялостна)

**Утвърдил:**

**Доц. д-р Добри Ярков**
**Ректор на Тракийски университет**

## 1. Въведение

Тази политика има за цел потвърди задължението на Тракийски университет (“организацията”) за опазването на обработваните от нея лични данни и гарантиране на правата на субектите, съгласно изискванията на Общ регламент за защита на лични данни (“регламентът”).

Според регламента 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, се определя като ЛИЧНИ ДАННИ.

Тази политика определя процедурите, които се следват при обработването на лични данни. Процедурите и принципите, изложени тук, се спазват по всяко време от организацията, нейните служители, изпълнители или други страни, които работят от нейно име.

Организацията се ангажира не само със съдържанието на регламента, но и с духа му и обръща голямо внимание на правилното, законосъобразно и справедливо третиране на всички лични данни, като се зачитат законните права, неприкосновеността на личния живот и доверието на всички лица и заинтересовани страни.

## 2. Принципи за защита на личните данни

Тази политика има за цел да гарантира спазването на регламента. Той определя следните принципи, които спазват всички страни, обработващи лични данни. Всички лични данни се:

2.1. обработват законно, справедливо и по прозрачен начин по отношение на субекта на данните;

2.2. събират за конкретни, изрични и законни цели и не се обработват по начин, който е несъвместим с тези цели; по-нататъшната обработка на архивиране за цели от обществен интерес, научни или исторически научноизследователски цели или статистически цели, не се считат за несъвместими с първоначалните цели;

2.3. поддържат адекватни, уместни и ограничени до това, което е необходимо във връзка с целите, за които се обработват;

2.4. точни и, когато е необходимо, актуализирани; предприемат се всички разумни стъпки, за да се гарантира, че личните данни, които са неточни, като се имат предвид целите, за които се обработват, се изтриват или отстраняват незабавно;

2.5. съхраняват във форма, която позволява идентифицирането на субектите на данни не по-

дълго от необходимото за целите, за които се обработват личните данни; личните данни могат да бъдат съхранявани за по-дълги периоди, доколкото личните данни ще бъдат обработвани единствено с цел архивиране за обществени интереси, научни или исторически научноизследователски цели или статистически цели, при условие че са изпълнени съответните технически и организационни мерки, изисквани от регламента, с цел защитата на правата и свободите на субекта на данните;
2.6. обработват по начин, който гарантира подходяща сигурност на личните данни, включително защита срещу неразрешена или незаконна обработка и срещу случайна загуба, унищожаване или повреда, като се използват подходящи технически или организационни мерки.

**3. Законна, справедлива и прозрачна обработка на личните данни**

Регламентът цели да гарантира, че личните данни се обработват законосъобразно, справедливо и прозрачно, без това да накърнява правата на субекта на данните. В регламента се посочва, че обработването на лични данни е законосъобразно, ако се прилага поне едно от следните условия:
3.1. субектът на данните е дал съгласие за обработването на личните му данни за една или повече конкретни цели;
3.2. обработването е необходимо за изпълнението на договор, на който лицето, за което се отнасят данните, е страна или за да предприеме стъпки по искане на субекта на данните преди сключването на договор;
3.3. обработването е необходимо за спазване на правно задължение, на което се подчинява администраторът;
3.4. обработването е необходимо за защита на жизненоважните интереси на субекта на данните или на друго физическо лице;
3.5. обработката е необходима за изпълнение на задача, изпълнявана в обществен интерес или при упражняване на публична власт на контролиращия орган;
3.6. обработването е необходимо за целите на легитимните интереси, преследвани от администратора или от трета страна, освен когато тези интереси са пренебрегнати от основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато обектът е дете.

**4. Обработвани лични данни за конкретни, изрични и законни цели**

4.1. Организацията събира и обработва личните данни, посочени в Част 21 на тази Политика. Това може да включва лични данни, получени директно от субектите на данни (например данни за контакт, използвани, когато обектът на данни комуникира с нас) и данни, получени от трети страни (например Агенции за подбор на персонала, Застрахователи, Служби по трудова медицина, Органи на държавната власт).
4.2. Организацията обработва лични данни само за конкретните цели, посочени в Част 21 на тази Политика (или за други цели, изрично разрешени от Регламента). Субектите на данни ще бъдат информирани за целите, за които обработваме личните им данни в момента, в който те се събират директно от тях или колкото е възможно по-скоро (не повече от един календарен месец) след събирането, в случай че данните са получени от трета страна.

**5. Адекватна, подходяща и ограничена обработка на лични данни**

Организацията събира и обработва лични данни само за и в степента, необходима за конкретната(ите) цел(и), за които е информирала субектите на данни, както е посочено в Част 4, по-горе.

**6. Точност на личните данни и поддържане на данни до дата**

Организацията гарантира, че всички събрани и обработени лични данни се поддържат точни и актуални. Точността на данните се проверява в момента, в който се събират и след това на планирани интервали. Когато се установят неточни или неактуални данни, незабавно се предприемат всички разумни стъпки, за да се изменят или заличат тези данни, според случая.

**7. Навременна обработка на лични данни**

Организацията не съхранява лични данни за по-дълго от необходимото във връзка с целите, за които тези данни първоначално са събрани и обработени. Когато данните вече не се изискват, всички разумни стъпки се предприемат, за да бъдат изтрити без забавяне.

**8. Защита при обработката на лични данни**

Организацията гарантира, че всички събрани и обработени лични данни са защитени от неразрешена или незаконна обработка и от случайна загуба, унищожаване или повреда. Допълнителни подробности относно мерките за защита на данните и организационните мерки, са дадени в части 22 и 23 от настоящата политика.

**9. Отговорност**

9.1. Длъжностното лице по защита на личните данни в Тракийски университет е Пламена Иванова.

9.2. Организацията води писмени вътрешни записи за събирането, притежаването и обработката на всички лични данни, *които* включват следната информация:

9.1.1. името и данните на Организацията, нейното Длъжностно лице по защита на личните данни и всички приложими администратори на данни от трети страни;

9.1.2. целите, за които Организацията обработва лични данни;

9.1.3. подробности за категориите лични данни, събрани, съхранявани и обработвани от Организацията и категориите данни, за които се отнасят тези лични данни;

9.1.4. подробности (и категории) на трети страни, които ще получават лични данни от Организацията;

9.1.5. подробности за всички прехвърляния на лични данни към страни извън ЕИП, включително всички механизми и предпазни мерки за сигурност;

9.1.6. подробности за това колко дълго ще бъдат задържани от Организацията личните данни;

9.1.7. подробни описания на всички технически и организационни мерки, предприети от организацията, за да се гарантира сигурността на личните данни.

**10. Оценка на риска по повод обработката на лични данни**

Организацията извършва оценки на въздействието върху личните данни, съгласно изискванията на регламента. Оценяването се контролира от Длъжностното лице по защита на личните данни в Организацията и се отнася до следните важни области:

10.1. Цел(и), за които се обработват лични данни, и операциите по обработка, които се извършват с тези данни;

10.2. Подробности за законните интереси, преследвани от Организацията;

10.3. Оценка на необходимостта и пропорционалността на обработката на данни по отношение на целта (целите), за която се обработва;

10.4. Оценка на рисковете за отделните субекти на данни;

10.5. Подробности за мерките, прилагани за минимизиране и управление на рисковете, включително предпазни мерки, сигурност на данните и други мерки и механизми за гарантиране на защитата на личните данни, достатъчни за доказване на съответствието с

регламента.

**11. Права на субекта на лични данни**

Регламентът определя следните права, приложими за субектите на данни:

11.1. правото да бъдете информирани;
11.2. правото на достъп;
11.3. правото на поправяне;
11.4. правото на заличаване (известно също като "правото да бъдеш забравен");
11.5. право на ограничаване на обработката;
11.6. правото на преносимост на данни;
11.7. правото на възражение;
11.8. права по отношение на автоматизираното вземане на решения и профилиране.

**12. Информиране на субектите за данни**

12.1. Организацията гарантира, че при събирането на лични данни е предоставена следната информация на всеки субект на данни:
12.1.1. подробности за Организацията, включително, но не само, самоличността на неговото Длъжностно лице по защита на личните данни;
12.1.2. целта / целите, за които се събират и се обработват личните данни (както е описано подробно в Част 21 на тази Политика) и правното основание, обосноваващо това събиране и обработка;
12.1.3. когато е приложимо, законните интереси, с които Организацията оправдава събирането и обработката на личните данни;
12.1.4. когато личните данни не се получават директно от субекта на данните, категориите на събраните и обработвани лични данни;
12.1.5. когато личните данни трябва да бъдат прехвърлени на една или повече трети страни, подробности за тези страни;
12.1.6. когато личните данни трябва да бъдат прехвърлени на трета страна, която се намира извън Европейското икономическо пространство ("ЕИП"), подробности за това прехвърляне, включително, но без да се ограничават до съществуващите гаранции (вж. част 24 от настоящото Политика за допълнителни подробности относно прехвърлянето на данни от трети държави);
12.1.7. подробности за продължителността на съхраняване на личните данни от Организацията (или, ако няма предварително определен период, подробности за това как ще бъде определена тази продължителност);
12.1.8. подробности за правата на субекта на данни съгласно регламента;
12.1.9. подробности за правото на субекта на данни да оттегли своето съгласие за обработката на личните данни по всяко време;
12.1.10. подробности относно правото на субекта на данните да подаде жалба до КЗЛД ("надзорният орган" съгласно регламента);
12.1.11. където е приложимо, подробности за всяко правно или договорно изискване или задължение, изискващо събирането и обработката на личните данни и подробности за последствията от непредоставянето им;
12.1.12. подробности за всяко автоматично вземане на решения, което се извършва, като се използват личните данни (включително, но не само профилирането), включително информация за това как се вземат решения, значението на тези решения и последствията от тях.
12.2. Информацията, посочена по-горе в Част 12.1, се предоставя на субекта на данните в следното приложимо време:
12.2.1. Когато личните данни са получени пряко от субекта на данните в момента на

събирането;
12.2.2. Когато личните данни не се получават пряко от субекта на данни (т.е. от друга страна):
- ако личните данни се използват за комуникация с лицето, за което се отнасят данните, по време на първото съобщение; или
- ако личните данни трябва да бъдат разкрити на друга страна, преди да бъдат разкрити личните данни; или
- във всеки случай не повече от един месец след датата, на която Организацията получава личните данни.

**13. Достъп до лични данни**

13.1. Даден субект на данните може по всяко време да направи заявка за достъп до своите лични данни ("ЗДД"), за да разбере повече информацията, която Организацията притежава за него. Организацията се стреми да отговори на ЗДД в рамките на един месец от получаването му (това може да бъде удължено с до два месеца в случай на сложни и/или многобройни искания, а в такива случаи субектът на данните е информиран за необходимостта от удължаване на срока.

13.2. Всички получени искания за достъп трябва да бъдат изпратени до Длъжностното лице по защита на личните данни в организацията. E-mail: vanya.trifonova@trakia-uni.bg, телефон: 042 699 206.

13.3. Организацията не начислява такса за обработка на нормални ЗДД, но си запазва правото да начислява разумни такси за допълнителни копия на вече предоставена информация на субекта на данни и за искания, които са явно неоснователни или прекомерни, особено когато такива искания се повтарят.

**14. Корекция на лични данни**

14.1. Ако даден субект на данни информира Организацията, че личните данни, съхранявани от нея, са неточни или непълни, като изисква те да бъдат коригирани, въпросните лични данни биват поправени и субектът на данните следва да бъде информиран за това коригиране в рамките на един месец от получаването на предупреждението му (това може да бъде удължено с до два месеца в случай на сложни искания, а в такива случаи субектът на данните трябва да бъде информиран за необходимостта от удължаване).

14.2. В случай, че всички засегнати лични данни са били разкрити на трети лица, тези страни трябва да бъдат информирани за всяка поправка на тези лични данни.

**15. Заличаване на лични данни**

15.1. Субектите на данни могат да поискат от Организацията да изтрие личните данни, които притежава за тях, при следните обстоятелства:

15.1.1. Вече не е необходимо Организацията да поддържа личните данни по отношение на целта, за която е била първоначално събрана или обработена;

15.1.2. Субектътна данните желае да оттегли своето съгласие за притежаване и обработване на личните му данни от Организацията;

15.1.3. Субектътна данните възразява срещу това, че Организацията притежава и обработва личните му данни (и няма преимуществен легитимен интерес, който да позволи на Организацията да продължи това) (вж. Част 18 от тези Политика за допълнителни подробности относно правото на субектите на данни да оспорят);

15.1.4. Личните данни са били обработени незаконно;

15.1.5. Личните данни трябва да бъдат изтрити, за да може Организацията да спазва конкретно правно задължение;

15.1.6. Личните данни се съхраняват и обработват с цел предоставяне на „услуга на

информационното общество“, което означава услуга по смисъла на член 1, параграф 1, точка б) от Директива (ЕС) 2015/1535 на Европейския парламент.
15.2. Освен ако Организацията има основателни причини да откаже да изтрие лични данни, всички молби за изтриване се спазват и субектът на данните се уведомява за изтриването в рамките на един месец от получаването на искането на субекта на данните (това може да бъде удължено до два месеца в случай на сложни искания, а в такива случаи субектът на данните се информира за необходимостта от удължаване).
15.3. В случай че лични данни, които трябва да бъдат изтрити в отговор на искане на субекта на данни, са били разкрити на трети лица, тези страни биват информирани за изтриването (освен ако това не е невъзможно или би изисквало несъразмерно усилие за това).

**16. Забрана за обработка на лични данни**
16.1. Субектите на данни могат да поискат Организацията да прекрати обработването на личните данни, които притежава за тях. Ако даден субект на данни направи такова искане, Организацията запазва само количеството лични данни, отнасящи се до този субект на данните, което е необходимо, за да се гарантира, че няма да се извършва по-нататъшна обработка на личните им данни.
16.2. В случай че всички засегнати лични данни са разкрити на трети лица, тези страни биват информирани за приложимите ограничения при обработването им (освен ако това не е невъзможно или би изисквало несъразмерно усилие за това).

**17. Преносимост на лични данни**
17.1. Организацията обработва лични данни чрез автоматизирани средства. Използва се софтуер от „Информационно обслужване“ АД - Пловдив и BeOnline Ltd., както и програмни продукти на „Ажур“ и „Омекс“ разработен за нуждите на Тракийски университет.
17.2. Когато субектите на данни дадат своето съгласие на Организацията да обработва личните им данни по такъв начин или обработването е необходимо за изпълнението на договор между Организацията и субекта на данните, субектите имат законовото право съгласно Регламента да получават копие от личните им данни и да ги използват за други цели (а именно да ги предават на други администратори на данни, например други организации).
17.3. За да се улесни правото на преносимост на данните, Организацията трябва да предостави всички приложими лични данни на субектите на данни в следния формат:
17.3.1. хартиен носител;
17.3.2. електронен вариант.
17.4. Когато това е технически осъществимо, при поискване от субект на данни, личните данни се изпращат директно на друг администратор на данни.
17.5. Всички заявки за копия на лични данни трябва да бъдат спазени в рамките на един месец от искането на субекта на данните (това може да бъде удължено с до два месеца в случай на сложни искания в случай на сложни или многобройни искания, а в такива случаи субектът на данни трябва да бъде информиран за необходимостта от удължаване).

**18. Възражения срещу обработката на лични данни**
18.1. Субектите на данни имат право да възразят срещу това, че Организацията обработва техни лични данни въз основа на законни интереси (включително профилиране), директен маркетинг (включително профилиране) и обработка за научни и/или исторически изследвания и статистически цели.
18.2. Когато даден субект на данни възразява срещу това, че Организацията обработва личните му данни въз основа на законните му интереси, Организацията незабавно прекратява

такава обработка, освен ако не може да се докаже, че законните основания на Организацията за такава обработка надвишават интересите, правата и свободите на субекта на данните; или обработването е необходимо за извършване на съдебни искове.
18.3. Когато даден субект на данни възразява срещу това, че Организацията обработва неговите лични данни за целите на директния маркетинг, Организацията незабавно прекратява такава обработка.
18.4. Когато даден субект на данни възразява срещу това, че Организацията обработва личните му данни за научни и/или исторически проучвания и статистически цели, субектът на данните трябва съгласно Регламента да "демонстрира основания, свързани с конкретната ситуация". Организацията не е задължена да се съобрази с това възражение, ако обработва данните от съображения за обществен интерес.

**19. Автоматично вземане на решения**

19.1. В случай, че Организацията използва лични данни за целите на автоматизираното вземане на решения и тези решения имат правен (или подобно значим) ефект върху субектите на данни, субектите на данни имат право да оспорят такива решения съгласно Регламента, като поискат намеса, изразяване на собствената си гледна точка и получаване на обяснение на решението на Организацията.
19.2. Правото, описано в Част 19.1 не се прилага при следните обстоятелства:
19.2.1. решението е необходимо за влизането или изпълнението на договор между Организацията и субекта на данните;
19.2.2. решението е разрешено от закона;
19.2.3. субектът на данните е дал своето изрично съгласие.

**20. Профилиране**

Когато Организацията използва лични данни за целите на профилирането:
20.1. се предоставя ясна информация, обясняваща профилирането, включително значението и вероятните последици;
20.2. използват се подходящи математически или статистически процедури;
20.3. въвеждат се технически и организационни мерки, необходими за минимизиране на риска от грешки и за да се позволи лесното коригиране на такива грешки; и
20.4. Всички лични данни, обработени с цел профилиране, трябва да бъдат обезопасени, за да се предотврати дискриминационното въздействие, произтичащо от профилиране (вж. части 22 и 23 от настоящата Политика за повече подробности относно сигурността на данните).

**21. Лични данни**

Типовете лични данни, съхранявани и обработвани от Организацията, са описани в Регистър на ЛД, чиято актуалност се контролира от Длъжностно лице по защита на данните.

**22. Мерки за защита на данните**

Организацията гарантира, че всички негови служители, контрагенти или други страни, работещи от негово име, отговарят на следното при работа с лични данни:
22.1. Всички имейли, съдържащи лични данни, са шифровани;
22.2. Когато някоя лична информация трябва да бъде изтрита или по друг начин да бъде изхвърлена по някаква причина (включително когато са направени копия и вече не са необходими), тя следва да бъде защитена и изхвърлена. Хартията бива нарязана като се използва шредер машина, а електронните копия се изтриват сигурно (формат на flash памет, HDD), оптичните дискове биват унищожавани механично.

22.3. Личните данни се предават само в защитени мрежи, предаването на данни по необезпечени мрежи не е разрешено при никакви обстоятелства;
22.4. Личните данни не могат да се предават чрез безжична мрежа, ако има жична алтернатива, която е разумно приложима;
22.5. Личните данни, съдържащи се в тялото на имейл, независимо дали са изпратени или получени, се копират от тялото на този имейл и да се съхраняват сигурно. Самият имейл се изтрива. Всички временни файлове, свързани с него също се заличават;
22.6. Когато личните данни трябва да бъдат изпратени чрез факсимилно предаване, получателят предварително бива информиран за предаването и да чака от факс машината да получи данните;
22.7. Когато личните данни трябва да бъдат прехвърлени на хартиен носител, те трябва да бъдат предадени директно на получателя или изпратени чрез пощенски услуги с помощта на Български пощи или куриерски фирми;
22.8. Никакви лични данни не могат да бъдат споделяни неофициално и ако служител, подизпълнител или друга страна, работеща от името на Организацията, изисква достъп до лични данни, до които те вече нямат достъп, този достъп трябва да бъде официално поискан от Ректора, e-mail: rector@uni-sz.bg, 042 699 202;
22.9. Всички хартиени копия на лични данни, както и всички електронни копия, съхранявани на физически, подвижни носители, се съхраняват сигурно в заключена кутия, чекмедже, шкаф или други подобни;
22.10. Никакви лични данни не могат да бъдат прехвърляни на служители, изпълнители или други страни, независимо дали тези лица работят от името на Организацията или не, без разрешение на Ректора, e-mail: rector@uni-sz.bg, 042 699 202;
22.11. Личните данни се обработват грижливо по всяко време и не се оставят без надзор или по преценка на неразрешени служители, подизпълнители или други страни по всяко време;
22.12. Ако се разглеждат лични данни на екрана на компютъра и въпросният компютър трябва да бъде оставен без надзор за определен период от време, потребителят заключва компютъра и екрана, преди да напусне компютъра;
22.13. Не се съхраняват лични данни на нито едно мобилно устройство (включително, но не само, лаптопи, таблети и смартфони).
22.14. Лични данни не се прехвърлят на каквото и да е устройство, принадлежащо на служител, и лични данни могат да се прехвърлят само на устройства, принадлежащи на изпълнители или други страни, работещи от името на Организацията, когато въпросната страна се е съгласила да спази изцяло с писмото и духа на тази Политика и на Регламента (което може да включва демонстриране пред Организацията, че са взети всички подходящи технически и организационни мерки);
22.15. Всички лични данни, съхранявани по електронен път, са архивирани със съхранени архиви в Тракийски университет и фирмите обслужващи софтуера („Информационно обслужване“ АД - Пловдив и BeOnline Ltd.). Всички архиви са шифровани, използвайки методи на криптиране.

В ИУИС се използват криптирани пароли за нуждите на автентификация на потребителите, управлявани автоматично от информационната система.

Паролите се генерират от псевдо случаен софтуерен генератор, имплементиран в ИУИС и се съхраняват от информационната система в криптиран вид.

Те не могат да бъдат възстановявани. При съмнение за компрометиране на паролата, тя се извежда от употреба и се заменя с нова.

ИУИС се намира на сървъри на Тракийски университет. Достъпа до базата данни и приложението е защитен със система от пароли.

За осигуряването на дистанционен достъп до ИУИС по интернет е необходимо да се използват протоколи с вградени криптиращи средства.

Таблицата на потребителите в Moodle съдържа: Username, Password, E-mail, City, Country, First name, Middle name, Last name, Address (опционално), Telephone (опционално).

Паролата е единственото поле, което се криптира. Методът, използван за криптиране се нарича bcrypt. Той генерира хаш и го записва в базата с данните. По този начин, дори и да бъде направена инжекция на базата с данни (рискът от това е минимален), паролите няма как да бъдат използвани директно.

За допълнителна сигурност има и метод, наречен salt. Той добавя произволни символи към края на хаша, което прави стандартизираните методи за декриптиране неизползваеми.

22.16. Всички електронни копия на лични данни се съхраняват сигурно, като се използват сложни пароли и криптиране на данните;

22.17. Всички пароли, използвани за защита на личните данни, се променят редовно и не могат да използват думи или фрази, които лесно могат да бъдат познавани или компрометирани по друг начин. Всички пароли съдържат комбинация от главни и малки букви, цифри и символи Всеки софтуер, използван от Организацията, изисква такива пароли;

22.18. При никакви обстоятелства пароли не се записват или се споделят между служители, изпълнители или други страни, работещи от името на Организацията, независимо от старшинството или отдела. Ако паролата е забравена, тя бива нулирана с помощта на приложимия метод. ИТ персоналът няма достъп до пароли.

## 23. Организационни мерки

Организацията гарантира, че са предприети следните мерки по отношение на събирането, притежаването и обработката на лични данни:

23.1. Всички служители, изпълнители или други страни, работещи от името на Организацията, са напълно запознати както със своите индивидуални отговорности, така и с отговорностите на Организацията съгласно Регламента и тази Политика и им се предоставя копие от тази Политика;

23.2. Само служители, подизпълнители или други лица, работещи от името на Организацията, които имат нужда от достъп и използване на лични данни, за да изпълняват правилно своите задачи, имат достъп до личните данни, съхранявани от Организацията;

23.3. Всички служители, изпълнители или други страни, работещи от името на Организацията, обработващи лични данни, биват подходящо обучени за това;

23.4. Всички служители, изпълнители или други страни, работещи от името на Организацията, работещи с лични данни, биват надлежно контролирани;

23.5. Методите за събиране, съхраняване и обработване на лични данни се оценяват и преглеждат редовно;

23.6. Работата на тези служители, агенти, изпълнители или други лица, работещи от името на Организацията, обработващи лични данни, редовно се оценява и преглежда;

23.7. Всички служители, изпълнители или други страни, които работят от името на Организацията, обработващи лични данни, са длъжни да го направят в съответствие с принципите на Регламента и настоящата Политика по договор;

23.8. Всички изпълнители или други лица, работещи от името на Организацията, обработващи лични данни, трябва да гарантират, че всички и всички техни служители, които участват в обработката на лични данни, се зачитат при същите условия, както съответните служители на Организацията произтичащи от тази политика и регламента;

23.9. Когато някой изпълнител или друга страна, работеща от името на Организацията, обработващ лични данни, не изпълни задълженията си по тази Политика, тази страна ще

обезщети и ще обезвреди Организацията срещу всички разходи, отговорност, вреди, загуби, искове или производства, възникнали от този провал.

## 24. Прехвърляне на лични данни извън Европейското икономическо пространство ЕИП

24.1. Организацията може в определени случаи да прехвърля ("прехвърляне" включва вземане на лични данни дистанционно) лични данни в страни извън ЕИП.

24.2. Прехвърлянето на лични данни в страна извън ЕИП се извършва само ако се прилагат едно или повече от следните условия:

24.2.1. Прехвърлянето е към страна, територия или един или повече специфични сектори в тази страна (или международна организация), които Европейската комисия е определила, гарантира адекватно ниво на защита на личните данни;

24.2.2. Прехвърлянето е към страна (или международна организация), която предоставя подходящи предпазни мерки под формата на правно обвързващо споразумение между публичните органи; обвързващи корпоративни правила; стандартните клаузи за защита на данните, приети от Европейската комисия; спазването на одобрен от надзорния орган кодекс за поведение (например КЗЛД); сертифициране по одобрен механизъм за сертифициране (както е предвидено в регламента); договорни клаузи, договорени и разрешени от компетентния надзорен орган; или разпоредби, въведени в административни договорености между публични органи или органи, упълномощени от компетентния надзорен орган;

24.2.3. Прехвърлянето се извършва с информирано съгласие на съответния (ите) субект (и) на данните;

24.2.4. Прехвърлянето е необходимо за изпълнението на договор между субекта на данни и Организацията (или за предприсъединителните мерки, предприети по искане на субекта на данни);

24.2.5. Прехвърлянето е необходимо поради важни причини от обществен интерес;

24.2.6. Прехвърлянето е необходимо за провеждане на съдебни искове;

24.2.7. Прехвърлянето е необходимо за защита на жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните физически или юридически не е в състояние да даде своето съгласие;

24.2.8. Прехвърлянето се извършва от регистър, който съгласно законодателството на Обединеното кралство или ЕС има за цел да предоставя информация на обществеността и който е отворен за достъп от страна на обществеността като цяло или по друг начин на тези, които са в състояние да демонстрират законния си интерес от достъп регистъра.

## 25. Уведомяване за нарушаване на личните данните

25.1. Всички нарушения на сигурността на лични данни се докладват незабавно на Длъжностното лице по защита на личните данни. Докладването се извършва според приетите канали за комуникация и докладване на ИКТ инциденти в организацията или директно.

25.2. Ако настъпи нарушение на лични данни и това нарушение е вероятно да доведе до риск за правата и свободите на субектите на данни (например финансови загуби, нарушаване на поверителността, дискриминация, вреди, причинени от репутацията или други значителни социални или икономически щети), Длъжностното лице по защита на личните данни е необходимо да гарантира, че КЗЛД е информирана за нарушението незабавно и при всички случаи в рамките на 72 часа след като е била уведомена за това.

25.3. В случай че нарушаването на личните данни е вероятно да доведе до висок риск (т.е. по-висок риск от този, описан в част 25.2) на правата и свободите на субектите на данни, Длъжностното лице по защита на личните данни е необходимо да гарантира, че всички засегнати данни субектите са информирани за нарушението директно и без неоправдано

забавяне.

25.4. Известията за нарушаване на данни включват следната информация:

- категориите и приблизителния брой на засегнатите субекти на данни;
- категориите и приблизителния брой записи на лични данни;
- името и данните за контакт на Длъжностното лице по защита на личните данни (или друго звено за контакт, където може да се получи повече информация);
- вероятните последици от нарушението;
- подробности за предприетите или предложени за предприемане мерки от страна на Организацията за справяне с нарушението, включително, когато е целесъобразно, мерки за смекчаване на евентуалните неблагоприятни последици.

## 26. Изпълнение на политиката

Настоящата Политика влиза в сила от 25.05.2018 г. и е актуализирана за последен път на 02.02.2021 г.

Нито една част от тази Политика няма да има обратно действие и следователно ще се прилага само за въпроси, настъпили на или след тази дата.