**ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА СЛУЖИТЕЛИТЕ, КЛИЕНТИ И ДОСТАВЧИЦИ НА "АРСЕНАЛ" АД,**

**в съответствие с изискванията на Регламент (ЕС) 2016/679**

**на Европейския парламент и Съвета – Общ Регламент за защитата**

**на личните данни (General Data Protection Regulation - GDPR)**

## 1. Въведение

Тази политика определя дейността на **"АРСЕНАЛ" АД, ЕИК 833067612**, регистрирано в Търговския регистър към Агенция по вписвания в Република България, чието седалище е гр. Казанлък 6100, ул. „Розова долина“ № 100, тел.: +359 431 63322, факс: +359 431 63332, електронна поща: arsenal@arsenal-bg.com, интернет страница: www. arsenal-bg.com, представлявано от управител НИКОЛАЙ ХРИСТОВ ИБУШЕВ, ("Дружеството") по отношение защитата на личните данни на служителите, клиентите и доставчиците ("субектите на данни") в съответствие с **Регламент (ЕС) 2016/679 – Общ Регламент за защита на личните данни (General Data Protection Regulation - GDPR).**

GDPR дефинира "лични данни" като всяка информация, отнасяща се до идентифицирано или подлежащо на идентификация физическо лице ("субект на данни"); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано пряко или непряко, по-специално чрез посочване на идентификатор като име, идентификационен номер, данни за местонахождението, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

Тази политика определя задълженията на Дружеството по отношение на събирането, обработката, прехвърлянето, съхранението и изтриването или унищожаването на лични данни, отнасящи се до служителите, клиентите и доставчиците. Процедурите и принципите, посочени тук, трябва да бъдат спазвани по всяко време от Дружеството, нейните служители, агенти, изпълнители или други страни, които работят от негово име.

Дружеството се ангажира не само с буквата на закона, но и с духа на закона и отдава голямо значение на правилното, законосъобразно и справедливо третиране на всички лични данни, като се зачитат законните права, неприкосновеността на личния живот и доверието на всички лицата, с които се занимава.

**2. Принципи за защита на данните**

Тази политика има за цел да гарантира спазването на GDPR. GDPR определя следните принципи, които трябва да спазва всяка страна, която обработва лични данни.

Личните данни трябва да бъдат:

2.1 Обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните.

2.2 Събирани за конкретни, изрично указани и легитимни цели и не се обработват по начин, който е несъвместим с тези цели; по-нататъшната обработка за целите на архивирането в интерес на обществото, за научни или исторически изследвания или статистически цели не се счита за несъвместима с първоначалните цели.

2.3 Адекватни, релевантни и ограничени до необходимото във връзка с целите, за които се обработват.

2.4 Точни и при необходимост актуализирани; трябва да се предприемат всички разумни стъпки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват.

2.5 Поддържани във форма, която позволява идентифицирането на субекта на данни за период не по-дълъг от необходимото за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги периоди от време, доколкото ще се обработват единствено с цел архивиране за обществени интереси, научни или исторически научноизследователски цели или за статистически цели, при условие че са изпълнени съответните технически и организационни мерки, изисквани от GDPR, за да се защитят правата и свободите на субекта на данните.

2.6. Обработвани по начин, който гарантира тяхната сигурност, включително защита срещу неразрешено или незаконно обработване и срещу случайна загуба, унищожаване или повреждане, като се използват подходящи технически или организационни мерки.

**3. Права на субектите на данни**

В своята дейност Дружеството съблюдава следните правила на субектите на данни в съответствие с изискванията на GDPR (за повече подробности направете справка в посочените в тази политика части):

3.1 Право на информация (Част 12)

3.2 Право на достъп (част 13)

3.3 Право на коригиране (Част 14)

3.4 Право за изтриване (известно също като "право да бъде забравено") (част 15)

3.5 Право на ограничаване на обработването (Част 16)

3.6 Право на преносимост на данни (Част 17)

3.7 Право на възражение (Част 18)

3.8 Права по отношение на автоматизираното вземане на решения и профилиране (Части 19 и 20).

**4. Законосъобразна, справедлива и прозрачна обработка на лични данни**

4.1 GDPR се стреми да гарантира, че личните данни се обработват законосъобразно, справедливо и прозрачно, без това да накърнява правата на субекта на данните. GDPR гласи, че обработването на лични данни е законосъобразно, ако се прилага поне едно от следните условия:

4.1.1 Субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

4.1.2 Обработването е необходимо за изпълнение на договор, по който субектът на данните е страна или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

4.1.3 Обработването е необходимо за спазване на правно задължение, на което се подчинява администраторът на данните;

4.1.4 Обработването е необходимо за защита на жизненоважните интереси на субекта на данните или на друго физическо лице;

4.1.5 Обработването е необходимо за изпълнение на задача, изпълнявана в обществен интерес или при упражняване на публична власт на администратора на данни;

4.1.6 Обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато такива интереси са надхвърлени от основните права и свободи на субекта на данните, които изискват защита на лични данни, по-специално когато субектът на данните е дете.

4.2 Администраторът не обработва лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и генетични данни, биометрични данни за целите единствено на идентифицирането на физическото лице, данни за здравословното състояние или данни за сексуалния живот или сексуална ориентация на физическото лице, ако не е изпълнено поне едно от следните условия:

4.2.1 Субектът на данни е дал своето изрично съгласие за обработването на тези данни за една или повече конкретни цели;

4.2.2 Обработването е необходимо за целите на легитимните интереси на администратора или на субекта на данните в областта на трудовото право, социалното осигуряване и правото на социална защита (доколкото е разрешено от ЕС или Законодателството на държавите-членки на ЕС или колективен трудов договор съгласно законодателството на държавите-членки на ЕС, който предвижда подходящи гаранции за основните права и интереси на субекта на данните);

4.2.3 Обработването е необходимо за защита на жизненоважните интереси на субекта на данните или на друго физическо лице, когато субектът на данните физически или юридически не е в състояние да даде съгласието си;

4.2.4 Администраторът на данни е фондация, асоциация или друг орган с нестопанска цел с политическа, философска, религиозна или синдикална цел и обработването се осъществява в хода на легитимните му дейности, при условие че обработката е свързана единствено на членовете или бившите членове на този орган или на лица, които имат постоянен контакт с него във връзка с неговите цели и че личните данни не се разкриват извън органа без съгласието на субектите на данни;

4.2.5 Обработването се отнася до лични данни, които явно са направени обществено достояние от субекта на данните;

4.2.6 Обработването е необходимо за извършване на съдебни искове или когато съдилищата действат в качеството си на съдебни служители;

4.2.7 Обработването е необходимо по причини от важен обществен интерес, въз основа на правото на ЕС или на държавите-членки на ЕС, което е пропорционално на преследваната цел, съблюдава същността на правото на защита на данните и предвижда подходящи и специфични мерки за защита на основните права и интереси на субекта на данните;

4.2.8 Обработването е необходимо за целите на превантивната или трудовата медицина, за оценка на работоспособността на служителя, за медицинска диагностика, за предоставяне на здравни или социални грижи или лечение или за управление на здравни или социални грижи системи или услуги въз основа на правото на ЕС или на държавите-членки на ЕС или съгласно договор със здравен специалист, при спазване на условията и предпазните мерки, посочени в член 9, параграф 3 от GDPR;

4.2.9 Обработването е необходимо от съображения от обществен интерес в областта на общественото здравеопазване, като например предпазване от сериозни трансгранични заплахи за здравето или осигуряване на високи стандарти за качество и безопасност на здравните грижи и на лекарствени продукти или медицински изделия, основа на законодателството на ЕС или на държавите-членки на ЕС, което предвижда подходящи и специфични мерки за защита на правата и свободите на субекта на данните (по-специално професионална тайна);

4.2.10 Обработването е необходимо за целите на архивирането в интерес на обществото, научните или историческите изследвания или статистическите в съответствие с член 89, параграф 1 от GDPR, основаващ се на правото на ЕС или на държавите-членки на ЕС, които са пропорционални на преследваната цел, съблюдават същността на правото на защита на данните и предвиждат подходящи и специфични мерки за защита на основните права и интересите на субекта на данните.

**5. Определени, изрични и законни цели**

5.1 Дружеството събира и обработва личните данни, посочени в Части 21 до 25 на тази Политика. Това включва:

5.1.1 Лични данни, събрани директно от работниците/служителите, клиентите и доставчиците (субекти на данните);

5.1.2 Лични данни, получени от трети страни.

5.2 Специфичните цели, за които Дружеството събира, обработва и съхранява такива лични данни, са посочени в Части 21-25 от тази Политика (или за други цели, изрично разрешени от GDPR).

5.3 Субектите на данни могат да се информират по всяко време за целта или целите, за които дружеството използва личните им данни (Виж част 12 за повече информация относно информирането на субектите на данни).

**6. Адекватна, подходяща и ограничена обработка на данни**

Дружеството събира и обработва лични данни само за и до степента, необходима за конкретната цел или целите, на които субектите на данни са били информирани или ще бъдат информирани (както е посочено в Част 5 по-горе и в Части 21 до 25, по-долу).

**7. Точност на данните и поддържане на данните актуални**

7.1 Дружеството гарантира, че всички обработвани лични данни се съхраняват точни и актуални. Това включва, но не ограничава коригирането на лични данни по искане на субекта на данните (Виж част 14 по-долу);

7.2 Точността на личните данни се проверява, когато се събира и в процеса на обработването. Ако се установи, че лични данни са неточни или не са актуални, незабавно се предприемат всички разумни стъпки, за да се изменят или изтрият тези данни, според случая.

**8. Запазване на данни**

8.1 Дружеството няма да съхранява лични данни за по-дълго от необходимото в съответствие с целта или целите, за които тези лични данни са били първоначално събрани, държани и обработени.

8.2 Когато личните данни повече не са необходими, администраторът предприема стъпки да бъдат изтрити или унищожени незабавно по друг начин;

8.3 За пълни подробности относно подхода на Дружеството към задържането на данни, включително периодите на запазване за конкретни типове лични данни, направете справка с правилата ни за съхранение на данни.

**9. Защитена обработка**

Дружеството гарантира, че всички събрани, съхранявани и обработвани лични данни са защитени от неразрешена или незаконна обработка и от случайна загуба, унищожаване или повреда (подробности за техническите и организационни мерки, които се предприемат, са дадени в Части от 26 до 31 от настоящата Политика).

**10. Отчетност и водене на записи**

10.1 Длъжностно лице за защита на личните данни на Дружеството е Стайко Христов, гр. Казанлък, ул. „Розова долина“ 100, П.К. 6100, тел: +359 431 63322 ; факс: +359 431 63332, електронен адрес: arsenal@arsenal-bg.com.

10.2 Длъжностното лице за защита на данните осъществява надзор и мониторинг на спазването на тази Политика, другите регламентиращи документи на Дружеството в областта на защитата на данните, както и на GDPR и другите приложими закони за защита на данните;

10.3 Дружеството води регистър на дейностите по обработването, който съдържа следната информация:

10.3.1 Името и координатите за връзка на Администратора и на длъжностното лице за защита на данните, както и всички приложими процеси за обработка на данни от трети страни;

10.3.2 Целите, за които Дружеството събира, съхранява и обработва лични данни;

10.3.3. Описание на субектите на данни и на категориите лични данни, събирани, обработвани и съхранявани от Дружеството;

10.3.4 Категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите от трети държави, включително всички механизми и предпазни мерки за сигурност;

10.3.5 Подробности за предвидените срокове за съхраняването на лични данни от Дружеството и сроковете за изтриване/унищожаване на различните категории данни;

10.3.6 Подробни описания на всички технически и организационни мерки, предприети от Дружеството, за да се гарантира сигурността на личните данни.

**11. Оценка на въздействието върху защитата на данните**

11.1 Дружеството ще извършва оценка на въздействието върху защитата на данните за всички нови проекти и/или нови приложения на лични данни, които включват използването на нови технологии и съответната обработка е вероятно да доведе до висок риск за правата и свободите на работниците и служителите;

11.2 Оценката на въздействието върху защитата на данните се прави от Администратора, като се иска становището на длъжностното лице за защита на данните. Тя включва:

11.2.1 Типа/типовете лични данни, които ще се събират, съхраняват и обработват;

11.2.2 Цел (и), за които трябва да се използват личните данни;

11.2.3 Целите на Дружеството;

11.2.4 Как трябва да се използват личните данни;

11.2.5 Страни (вътрешни и / или външни), с които да се провеждат консултации;

11.2.6 Необходимостта и пропорционалността на обработката на данни по отношение на целта / целите, за която (които) се обработва;

11.2.7 Рискове, наложени на субектите на данни;

11.2.8 Рискове, породени както от Дружеството, така и за него;

11.2.9 Предложени мерки за свеждане до минимум на идентифицираните рискове.

**12. Информиране на субектите за данни**

12.1 Дружеството предоставя информацията, посочена в Част 12.2, на всеки субект на данни:

12.1.1. Когато личните данни се събират директно от субектите на данни, те ще бъдат информирани за целта им по време на събирането;

12.1.2 Когато лични данни се получават от трета страна, съответните лица на данни ще бъдат информирани за целта им:

а) ако личните данни се използват за комуникация със субекта на данни - когато е направено първото съобщение;

б) ако личните данни трябва да бъдат прехвърлени на друга страна - преди да се извърши това прехвърляне;

в) възможно най-бързо и във всеки случай не повече от един месец след получаването на личните данни.

12.2 Предоставя се следната информация:

12.2.1 Данни за Дружеството, включително, но не само, самоличността на неговото длъжностно лице за защита на данните;

12.2.2 Цел (и), за които се събират и ще се обработват личните данни (както е описано подробно в Части 21-25 от настоящата Политика) и правното основание, обосноваващо това събиране и обработване;

12.2.3 Където е приложимо, законните интереси, въз основа на които Дружеството оправдава събирането и обработването на личните данни;

12.2.4 Когато личните данни не се получават директно от работниците и служителите, категориите събрани и обработени лични данни;

12.2.5 Когато личните данни трябва да бъдат прехвърлени на една или повече трети страни, подробности за тези страни;

12.2.6 Когато личните данни трябва да бъдат прехвърлени на трета страна, която се намира извън Европейското икономическо пространство ("ЕИП"), подробности за това прехвърляне, включително, но не само, съществуващите гаранции (виж Част 32 от тази политика за допълнителни подробности);

12.2.7 Подробности за запазването на личните данни;

12.2.8 Подробности за правата на субекта на данни по Регламент (ЕС) 2016/679;

12.2.9 Подробности за правото на субект на данни да оттегли своето съгласие за обработване на личните данни от Дружеството;

12.2.10 Подробности за правото на субекта на данните да подават жалби в надзорният орган – Комисията за защита на личните данни;

12.2.11 Където е приложимо, подробности за всяко правно или договорно изискване или задължение, изискващи събирането и обработването на личните данни и подробности за последствията от непредоставянето им;

12.2.12 Подробности за всяко автоматично вземане на решения или профилиране, което ще се осъществи, като се използват личните данни, включително информация за начина на вземане на решения, значението на тези решения и последствията от тях.

**13. Достъп до данни**

13.1 Лицата, чиито данни се обработват могат да направят заявки за достъп до обектите по всяко време, за да научат повече за личните данни, които Дружеството държи за тях, какво правят с тези лични данни и защо.

13.2 Лицата, чиито данни се обработват, трябва да използват формуляра за заявка за достъп до данни, като изпращат формуляра на длъжностното лице за защита на данните (виж част 10.1).

13.3 Отговорите обикновено се дават в рамките на един месец от получаването им, но това може да бъде удължено с до два месеца, ако достъпът до данни е сложен и/или са направени многобройни искания. Ако се изисква такова допълнително време, субектът на данните трябва да бъде информиран.

13.4 Всички получени формуляри за заявка за достъп до данни се обработват от длъжностното лице за защита на данните.

13.5 Дружеството не начислява такса за обработка на нормални заявки. Дружеството си запазва правото да начислява разумни такси за допълнителни копия на вече предоставена информация на субект на данни и за искания, които са явно неоснователни или прекомерни, особено когато тези искания са повтарящи се.

**14. Поправяне на лични данни**

14.1 Субектите на данни имат право да изискват от Дружеството да коригира всякакви лични данни, които са неточни или непълни.

14.2 Дружеството трябва да коригира или допълни въпросните лични данни и да информира субектите, които са предмет на тази корекция, в рамките на един месец от уведомяване на дружеството за въпросната информация. Периодът може да бъде удължен с до два месеца при сложни искания. Ако се изисква такова допълнително време, субектът на данните трябва да бъде информиран.

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

**15. Изтриване на лични данни**

15.1 Субектите на данни имат право да поискат от Администратора да изтрият личните данни, които притежава за тях, при следните обстоятелства:

15.1.1 Вече не е необходимо фирмата да съхранява личните данни по отношение на целта/целите, за която (които) първоначално са били събрани или обработени;

15.1.2 Субектът на данни желае да оттегли своето съгласие за обработване на личните му данни от дружеството;

15.1.3 Субектът на данни възразява срещу това, че Дружеството притежава и обработва личните му данни (и няма преимуществен законен интерес, за да позволи на Дружеството да продължи това) (виж Част 18 от тази Политика);

15.1.4 Личните данни са били обработени незаконосъобразно;

15.1.5 Личните данни трябва да бъдат изтрити, за да може Дружеството да спази определено правно задължение.

15.2 Освен ако Дружеството има основателни причини да откаже да изтрие личните данни, всички молби за изтриване трябва да бъдат спазени, а субекта на данни е уведомен за изтриването в рамките на един месец от получаването на искането. Периодът може да бъде удължен с до два месеца при сложни искания. Ако се изисква такова допълнително време, субектът на данните трябва да бъде информиран.

15.3 В случай, че лични данни, които трябва да бъдат изтрити в отговор на искане на субект на данни, са били разкрити на трети лица, тези страни трябва да бъдат информирани за изтриването (освен ако това не е невъзможно или би изисквало несъразмерно усилие за това).

**16. Ограничаване на обработването на лични данни**

16.1 Субектите на данни могат да поискат Дружеството да прекрати обработването на личните данни, които притежава за тях. Ако даден субект на данни отправи такова искане, Дружеството ще запази само количеството лични данни, отнасящи се до съответното физическо лице (ако има такива), което е необходимо, за да се гарантира, че въпросните лични данни не се обработват допълнително.

16.2 В случай, че всички засегнати лични данни са разкрити на трети лица, тези страни трябва да бъдат информирани за приложимите ограничения при обработването им (освен ако това не е невъзможно или би изисквало несъразмерно усилие за това).

**17. Преносимост на данни**

17.1 Дружеството обработва лични данни, свързани със служителите, използвайки автоматизирани средства.

17.2 Когато субектите на данни дадат своето съгласие на Дружеството да обработва личните им данни по такъв начин, или обработката е иначе необходима за

изпълнението на договор между Компанията и субекта на данни, субектите на данни имат право да получават копие от личните си данни и да ги използват за други цели (а именно да ги предават на други администратори на данни).

17.3 За улесняване правото на преносимост на данните, Дружеството предоставя всички приложими лични данни на субектите на данни в поискания вид/формат.

17.4 Когато това е технически осъществимо, при поискване от субект на данни, личните данни се изпращат директно до посочения 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 данни. Периодът може да бъде удължен с до два месеца в случай на сложни или многобройни искания. Ако се изисква такова допълнително време, субектът на данните трябва да бъде информиран.

**18. Възражения срещу обработването на лични данни**

18.1 Субектите на данни имат право да възразят срещу това, че Дружеството обработва личните данни въз основа на законови интереси, включително профилиране и срещу обработка за научни и / или исторически изследвания и статистически цели.

18.2 Когато даден субект на данни възразява срещу това, че Дружеството обработва личните му данни въз основа на законните му интереси, Дружеството незабавно преустановява такава обработка, освен ако не може да се докаже, че законните основания за такава обработка надвишават интересите, и свободата, или че обработването е необходимо за извършване на правни искове.

18.3 Когато даден субект на данни на служител възразява срещу това, че Дружеството обработва личните си данни за целите на директния маркетинг, Дружеството незабавно прекратява такава обработка.

18.4 Когато даден субект на данни възразява срещу това, че Дружеството обработва личните му данни за научни и/или исторически проучвания и статистически цели, субектът на данни трябва да демонстрира основанията, свързани с конкретната ситуация. Дружеството не е задължено да спазва, ако изследването е необходимо за изпълнението на задача, изпълнявана от съображения за обществен интерес.

**19. Автоматизирано вземане на решения**

19.1 Дружеството използва лични данни в автоматизирани процеси на вземане на решения по отношение на своите служители.

19.2 Когато такива решения имат законно (или подобно съществено въздействие) върху субектите на данни за служителите, те имат право да оспорят такива решения, като искат човешка намеса, изразяват своята гледна точка и получават обяснение за решението на Дружеството.

19.3 Правото, описано в Част 19.2, не се прилага при следните обстоятелства:

19.3.1 Решението е необходимо за влизането или изпълнението на договор между Дружеството и субекта на данните;

19.3.2 Решението е разрешено от закона;

19.3.3 Субектът на данните е дал своето изрично съгласие.

**20. Профилиране**

20.1 Дружеството използва лични данни за целите на профилирането по отношение на своите служители.

20.2 Когато се използват лични данни за целите на профилирането, се прилага следното:

20.2.1 Трябва да се предостави ясна информация, обясняваща профилирането, на субектите на данни, включително значението и вероятните последици от профилирането;

20.2.2 Използват се подходящи математически или статистически процедури;

20.2.3 Изпълняват се технически и организационни мерки за свеждане до минимум на риска от грешки. Ако възникнат грешки, такива мерки трябва да позволяват лесното им коригиране;

20.2.4 Всички лични данни, обработвани за целите на профилирането, трябва да бъдат обезпечени, за да се предотвратят дискриминационни ефекти, произтичащи от профилиране (виж Части 26-30 от настоящата Политика за повече подробности относно сигурността на данните).

**21. Лични данни**

Дружеството държи лични данни, които са пряко свързани с неговите служители. Личните данни се събират, съхраняват и обработват в съответствие с правата на субектите на данни и задълженията на Дружеството по GDPR и тази Политика. Дружеството може да събира, съхранява и обработва личните данни, описани подробно в Части 21 до 25 на тези Политика:

21.1 Идентификационна информация за служителите:

21.1.1 Имена;

21.1.2 Данни за връзка.

21.2 Информация за мониторинг на равни възможности (когато е възможно, тази информация се анонимира):

21.2.1 Възраст;

21.2.2 Пол;

21.2.3 Етническа принадлежност;

21.2.4 Националност;

21.2.5 Религия.

21.3 Здравни досиета (виж част 22, по-долу, за допълнителна информация):

21.3.1 Данни за отпуск по болест;

21.3.2 Медицински условия;

21.3.3 Увреждания;

21.3.4 Предписано лекарство.

21.4 Записи по заетостта:

21.4.1 Бележки по интервюто;

21.4.2 Автобиографии, формуляри за кандидатстване, придружителни писма и други подобни документи;

21.4.3 Оценки, прегледи на ефективността и други подобни документи;

21.4.4 Данни за възнаграждението, включително заплати, увеличения на заплатите, бонуси, комисионни, извънреден труд, обезщетения и разходи;

21.4.5 Подробности за членството в профсъюзите (виж част 24, по-долу, за допълнителна информация);

21.4.6 Информация за мониторинг на служителите (виж част 25, по-долу, за допълнителна информация);

21.4.7 Протоколи за дисциплинарни въпроси, включително доклади и предупреждения, официални и неформални;

21.4.8 Подробности за жалбите, включително документални доказателства, бележки от интервюта, следвани процедури и резултати.

**22. Здравни досиета**

22.1 Дружеството притежава здравни досиета на субектите на данни, които се използват за оценка на здравето и благосъстоянието на служителите и за изясняване на всички въпроси, които могат да изискват по-нататъшно разследване. По-специално, Дружеството поставя висок приоритет в поддържането на здравето и безопасността на работното място, насърчаването на равните възможности и предотвратяването на дискриминацията на основата на увреждане или други медицински състояния. В повечето случаи здравните данни за служителите попадат в специалните категории данни. Поради това всички данни, свързани със здравето на субектите на данните, ще бъдат събирани, съхранявани и обработвани стриктно в съответствие с условията за обработка на лични данни от специална категория, както е посочено в част 4 на тези Политика. Лични данни от специална категория няма да се събират, съхраняват или обработват без изричното съгласие на съответното физическо лице.

22.2 Здравните досиета са достъпни и използвани само от служба „Трудова медицина“ и не се разкриват на други служители, агенти, изпълнители или други страни, работещи от името на Дружеството без изрично съгласие на субекта (лицата) на данните, за които се отнасят тези данни, освен в изключителни случаи, когато благосъстоянието на субекта на данните, за който се отнасят данните, е изложено на риск и такива обстоятелства отговарят на едно или повече от посочени в част 4.2 от настоящата Политика.

22.3 Здравните досиета се събират, съхраняват и обработват само до степента, необходима, за да се гарантира, че служителите могат да извършват работата си правилно, законно, безопасно и без незаконни или несправедливи пречки или дискриминация.

22.4 Субектите на данни имат право да поискат от Дружеството да не води здравни досиета за тях. Всички такива искания трябва да бъдат изпратени в писмен вид и адресирани до длъжностното лице по защита на данни (виж част 10.1).

**23. Ползи**

23.1 В случаите, когато субектите на данни са записани в схеми за обезщетения, които се предоставят от Дружеството, от време на време може да е необходимо за организации на трети страни да събират лични данни от съответните субекти на данни.

23.2 Преди събирането на такива данни субектите на данни ще бъдат напълно информирани за личните данни, които трябва да бъдат събрани, причините за тяхното събиране и начина, по който ще бъдат обработвани, в съответствие с изискванията за информация посочени в част 12 от настоящата Политика.

23.3 Дружеството няма да използва такива лични данни, освен доколкото са така необходими за администрирането на съответните схеми за обезщетения.

**24. Синдикати**

24.1 Дружеството ще предостави на добросъвестни синдикати лични данни относно съответните субекти на данни, когато тези съюзи са признати от Дружеството. В повечето случаи информацията за членството в синдикатите на отделните лица попада в дефиницията на GDPR за специални категории данни (виж Част 4 от настоящата Политика). Всички данни, свързани с членството в синдикатите на данни за служителите, ще бъдат събирани, съхранявани и обработвани стриктно в съответствие с условията за обработка на лични данни от специална категория. Лични данни от специална категория няма да се събират, съхраняват или обработват без изричното съгласие на съответното лице. Ще бъдат събрани и предоставени следните данни:

24.1.1 Имена;

24.1.2 Описание на длъжността;

24.1.3 Първите шест цифри от ЕГН на субектите на данни, когато същите са заявили желание да кандидатстват за хотелско настаняване, в съответната почивна станция/хотел и следва да им се изготвят карти за настаняване.

24.2 Всички субекти на данни имат право да изискат, че Дружеството не предоставя личните им данни на синдикатите и ще бъде информирано за това право, преди да бъде направено такова прехвърляне.

**25. Мониторинг на субектите на данните**

25.1 Дружеството може периодично да наблюдава дейностите на субектите на данни. Такъв мониторинг може да включва, но не непременно да се ограничава до

интернет и електронно наблюдение. В случай, че трябва да се извърши мониторинг от всякакъв вид (освен ако изключителни обстоятелства, като например разследване на престъпна дейност или въпрос с еднаква тежест, оправдават скрит мониторинг), субектите на данни ще бъдат информирани за точния характер на мониторинга предварително.

25.2 Наблюдението не следва (освен ако изключителни обстоятелства го оправдават, както по-горе) да се намесва в нормалните задължения на служителя.

25.3 Наблюдението ще се извършва само ако Дружеството счита, че е необходимо да се постигне ползата, която е предназначена да се постигне. Личните данни, събрани по време на всяко такова наблюдение, ще бъдат събирани, съхранявани и обработвани само по причини, пряко свързани с (и необходими за) постигането на планирания резултат и по всяко време, в съответствие с правата на субектите на данни.

25.4 Дружеството трябва да гарантира, че няма ненужно навлизане на личните комуникации или дейности на субектите на данни и при никакви обстоятелства мониторингът няма да се извършва извън обичайното работно място на работното лице или работното време, освен ако съответното лице, използва фирмено оборудване или други съоръжения, включително, но не само, имейл на фирмата, фирмен интранет или виртуална частна мрежа, предоставяна от дружеството за използване от служителите.

**26. Сигурност на данните - Прехвърляне на лични данни и съобщения**

Дружеството гарантира, че са предприети следните мерки по отношение на всички комуникации и други трансфери, включващи лични данни (включително, но не само, лични данни, свързани със служителите):

26.1 Всички имейли, съдържащи лични данни, трябва да бъдат шифровани използвайки SHA-256 алгоритъм на криптиране;

26.2 Всички имейли, съдържащи лични данни, трябва да бъдат обозначени като "поверителни";

26.3 Личните данни могат да се предават само чрез защитени мрежи; предаването на данни по необезпечени мрежи не е разрешено при никакви обстоятелства;

26.4 Личните данни не могат да се предават чрез безжична мрежа, ако има разумно приложима алтернатива;

26.5 Личните данни, съдържащи се в имейл, независимо дали са изпратени или получени, трябва да се копират от тялото на този имейл и да се съхраняват сигурно. Самият имейл трябва да бъде изтрит. Всички временни файлове, свързани с него, също трябва да бъдат изтрити;

26.6 Когато личните данни трябва да бъдат изпратени чрез факсимилно предаване, получателят трябва предварително да бъде информиран за предаването и трябва да чака от факс машината да получи данните;

26.7 Когато личните данни трябва да се предават на хартиен носител, те трябва да бъдат предадени директно на получателя или изпратени с помощта на куриер, с

който Администраторът е договорно обвързан и носи отговорност за неразпространение на поверителна информация, в това число и лични данни;

26.8 Всички лични данни, които трябва да бъдат прехвърлени физически, независимо дали са на хартиен носител или на подвижни електронни носители, се прехвърлят в подходящ контейнер, обозначен като "поверителен".

**27. Сигурност на данните - съхранение**

Дружеството гарантира, че са предприети следните мерки по отношение на съхраняването на лични данни (включително, но не само, лични данни, свързани със служителите):

27.1 Всички електронни копия на лични данни трябва да се съхраняват сигурно, като се използват пароли и криптиране на данните;

27.2 Всички хартиени копия на лични данни, както и всички електронни копия, съхранявани на физически, подвижни носители, трябва да се съхраняват сигурно в заключена кутия, чекмедже, шкаф или други подобни;

27.3 Всички лични данни, съхранявани по електронен път, трябва да бъдат архивирани ежедневно със съхранени архиви на място и на отделен физически носител. Всички архиви трябва да бъдат шифровани;

27.4 Не трябва да се съхраняват лични данни на нито едно мобилно устройство (включително, но не само, лаптопи, таблети и смартфони), независимо дали такова устройство принадлежи на Компанията или по друг начин, без официално писмено одобрение на съответния ръководител на отдел и в случай на такова одобрение, стриктно в съответствие с всички указания и ограничения, описани в момента на издаване на одобрението, и не повече от абсолютно необходимото;

27.5 Лични данни не трябва да се прехвърлят на каквото и да е устройство, което е част от служител, и лични данни могат да бъдат прехвърляни само на устройства, принадлежащи на агенти, изпълнители или други страни, работещи от името на Дружеството, когато въпросната страна се е съгласила напълно да спази писмото и духа на тази политика и на GDPR (което може да включва демонстриране пред Дружеството, че са предприети всички подходящи технически и организационни мерки).

**28. Сигурност на данните - изхвърляне**

Когато всички лични данни трябва да бъдат изтрити или изхвърлени по друг начин по каквато и да е причина (включително когато са направени копия и вече не са необходими), те трябва да бъдат напълно заличени и унищожени. (За допълнителна информация относно заличаването и ликвидирането на лични данни, моля, направете справка с Правилата за запазване на данни на компанията).

**29. Сигурност на данните - използване на лични данни**

Дружеството гарантира, че са предприети следните мерки по отношение на използването на лични данни:

29.1 Никакви лични данни не могат да бъдат споделяни неофициално и ако служител, агент, подизпълнител или друга страна, работеща от името на Дружеството, изисква достъп до лични данни, до които те вече нямат достъп, този достъп трябва да бъде формално поискан от длъжностното лице за защита на данните (виж част 10.1);

29.2 Никакви лични данни не могат да бъдат прехвърляни на служители, агенти, изпълнители или други лица, независимо дали тези страни работят от името на Дружеството или не, без разрешение на длъжностното лице за защита на данните (виж част 10.1);

29.3 Личните данни трябва да се обработват с грижа по всяко време и не трябва да бъдат оставяни без надзор;

29.4 Ако се разглеждат лични данни на компютърния екран и въпросният компютър трябва да остане без надзор за определен период от време, потребителят трябва да заключи компютъра и екрана, преди да напусне компютъра.

**30. Сигурност на данните - ИТ сигурност**

Дружеството гарантира, че са предприети следните мерки по отношение на ИТ и информационната сигурност:

30.1 Всички пароли, използвани за защита на личните данни, трябва да се променят редовно и не трябва да използват думи или фрази, които лесно могат да бъдат познати или компрометирани по друг начин. Всички пароли трябва да съдържат комбинация от главни и малки букви, цифри и символи;

30.2 При никакви обстоятелства пароли не трябва да се записват или да се споделят между служители, агенти, изпълнители или други страни, които работят от името на Дружеството, независимо от старшинството или отдела. Ако паролата е забравена, тя трябва да бъде нулирана чрез приложимия метод. ИТ персоналът няма достъп до пароли;

30.3 Всички софтуерни продукти (включително, но не само, приложения и операционни системи) се актуализират. ИТ персоналът на Компанията отговаря за инсталирането на всички актуализации, свързани със сигурността, след като актуализациите се предоставят от издателя или производителя възможно най-бързо и практически възможно освен ако няма основателни технически причини да не се направи това;

30.4 Не може да се инсталира софтуер на нито един компютър или устройство, собственост на компанията, без предварителното одобрение на ръководителя на отдела/направлението.

**31. Организационни мерки**

Дружеството гарантира, че са взети следните мерки по отношение на събирането, притежаването и обработването на лични данни:

31.1 Всички служители, агенти, изпълнители или други страни, които работят от името на Дружеството, трябва да бъдат напълно запознати както с техните

индивидуални отговорности, така и с отговорностите на Дружеството съгласно GDPR и съгласно тази Политика;

31.2 Само лицата, агентите, подизпълнителите или други лица, работещи от името на Дружеството, които се нуждаят от достъп и ползване на лични данни, за да изпълняват правилно своите задачи, имат достъп до лични данни, съхранявани от Дружеството;

31.3 Всички служители, агенти, изпълнители или други лица, работещи от името на Дружеството, обработващи лични данни, ще бъдат обучени по подходящ начин за това;

31.4 Всички служители, агенти, изпълнители или други страни, работещи от името на Дружеството, обработващи лични данни, ще бъдат надлежно контролирани;

31.5 Всички служители, агенти, изпълнители или други страни, работещи от името на Дружеството, работещи с лични данни, се задължават да полагат грижи, предпазливост и дискретност, когато обсъждат въпроси, свързани с работата, свързани с лични данни, независимо дали на работното място или в противен случай;

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

31.7 Всички лични данни, съхранявани от Дружеството, се преглеждат периодично, както е посочено в Политиката за запазване на данни на компанията;

31.8 Изпълнението на тези служители, агенти, изпълнители или други лица, работещи от името на Дружеството, обработващи лични данни, трябва редовно да се оценява и преглежда;

31.9 Всички служители, агенти, изпълнители или други страни, които работят от името на Дружеството, обработващи лични данни, са длъжни да го направят в съответствие с принципите на GDPR и тази политика по договор;

31.10 Всички агенти, изпълнители или други страни, работещи от името на Дружеството, обработващи лични данни, трябва да гарантират, че всички и всички техни служители, които участват в обработката на лични данни, се държат при същите условия, както тези съответни служители на Дружеството от тази политика и GDPR;

31.11 Когато някой агент, изпълнител или друга страна, работещ от името на Дружеството, обработващ лични данни, не изпълни задълженията си по тази Политика, тази страна ще обезщети и ще обезвреди Дружеството срещу всякакви разходи, отговорност, вреди, загуби, искове или производства, които могат да възникнат от този неуспех.

**32. Предаване на лични данни в страна извън ЕИП**

32.1 Дружеството може от време на време да предава лични данни на страни извън ЕИП.

32.2 Предаването на лични данни в страна извън ЕИП се извършва само ако се прилагат едно или повече от следните условия:

32.2.1 Предаването е към страна, територия или един или повече специфични сектори в тази страна (или международна организация), за които Европейската комисия е определила, че осигурява адекватно ниво на защита на личните данни;

32.2.2 Предаването е към страна (или международна организация), която осигурява подходящи предпазни мерки под формата на правно обвързващо споразумение между държавните органи или органи, обвързващи корпоративни правила; стандартните клаузи за защита на данните, приети от Европейската комисия; спазването на одобрен от надзорния орган кодекс за поведение; сертифициране по одобрен механизъм за сертифициране (както е предвидено в GDPR); 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;

32.2.3 Предаването се извършва с информирано съгласие на съответния (ите) субект (и) на данните;

32.2.4 Предаването е необходимо за изпълнението на договор между субекта на данни и Дружеството (или за предприсъединителните мерки, предприети по искане на субекта на данни);

32.2.5 Предаването е необходимо поради важни причини от обществен интерес;

32.2.6 Предаването е необходимо за извършване на съдебни искове;

32.2.7 Предаването е необходимо, за да се защитят жизненоважните интереси на субекта на данни или на други лица, когато физическото или юридическото лице не е в състояние да даде своето съгласие;

32.2.8 Предаването се извършва от регистър, който съгласно правото на Съюза или правото на държавите членки е предназначен да предоставя информация на обществеността и който е достъпен за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, но само доколкото условията за справка, установени в правото на Съюза или правото на държавите членки, са изпълнени в конкретния случай.

**33. Уведомяване за нарушаване на данните**

33.1 Всички нарушения на лични данни трябва да бъдат съобщени незабавно на длъжностното лице за защита на данните.

33.2 Ако се случи нарушение на лични данни и това нарушение има вероятност да доведе до риск за правата и свободите на субектите на данни (напр. финансови загуби, нарушаване на поверителността, дискриминация, репутационни щети или други значителни социални или икономически щети), длъжностното лице за защита на данните трябва да гарантира, че Комисията за защита на личните данни е информирана незабавно за нарушението и при всички случаи в рамките на 72 часа след като е узнал за него.

33.3 В случай че нарушаването на личните данни е вероятно да доведе до висок риск (т. е. по-висок риск от този, описан в част 29.2) на правата и свободите на

субектите на данни, длъжностното лице за защита на данните трябва да гарантира, че всички засегнати субектите на данни са информирани за нарушението директно и без неоснователно забавяне.

33.4 Известията за нарушаване на данни включват следната информация:

33.4.1 Категориите и приблизителния брой на засегнатите субекти на данни за служителите;

33.4.2 Категориите и приблизителния брой записи на лични данни;

33.4.3 Името и данните за контакт на длъжностното лице за защита на данните (или друго звено за контакт, където може да се получи повече информация);

33.4.4 Вероятните последици от нарушението;

33.4.5 Подробности за взетите или предложени за предприемане мерки от страна на Дружеството за справяне с нарушението, включително, когато е целесъобразно, мерки за смекчаване на евентуалните неблагоприятни последици.

**34. Изпълнение на политиката**

Настоящата Политика се счита за влязла в сила от 25.05.2018 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.

Тази политика е одобрена от:

Име: Николай Христов Ибушев

Позиция: Изпълнителен директор