ПОЛИТИКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА СЛУЖИТЕЛИТЕ, КЛИЕНТИ И ДОСТАВЧИЦИ

на "АРСЕНАЛ" АД, ЕИК 833067612

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

(General Data Protection Regulation - GDPR)

1. Въведение

Тези Политики определят задълженията 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 No 100, тел.: 0431 6 33 22, факс: 0431 6 33 22, електронна поща: arsenal@arsenal-bg.com, интернет страница: www.arsenal-bg.com представлявано от управител НИКОЛАЙ ХРИСТОВ ИБУШЕВ, ("Компанията") по отношение на защитата на данните и правата на служителите, клиентите и доставчиците (в този контекст, "субектите на данни") по отношение на техните лични данни съгласно **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 човек, който може да бъде идентифициран пряко или непряко, по-специално чрез посочване на идентификатор като име, идентификационен номер, данни за местоположението, онлайн идентификатор или един или повече фактори, специфични за физическото, физиологичното , генетична, умствена, икономическа, културна или социална идентичност на това физическо лице.

Тази политика определя задълженията на компанията по отношение на събирането, обработката, прехвърлянето, съхранението и изхвърлянето на лични данни, отнасящи се до субектите на данни за служителите, клиенти и доставчици. Процедурите и принципите, посочени тук, трябва да бъдат спазвани по всяко време от Компанията, нейните служители, агенти, изпълнители или други страни, които работят от името на Дружеството.

Дружеството се ангажира не само с буквата на закона, но и с духа на закона и поставя голямо значение за 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. Принципите за защита на данните

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

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

2.2 Събрани за конкретни, изрични и законни цели и не се обработват по начин, който е несъвместим с тези цели. По-нататъшната обработка за целите на архивирането в интерес на обществото, научните или историческите научни цели или статистическите цели не се счита за несъвместима с първоначалните цели.

2.3 Адекватна, релевантна и ограничена до това, което е необходимо във връзка с целите, за които се обработва.

2.4 Точни и, ако е необходимо, актуализирани. Трябва да се предприемат 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 коригират незабавно.

2.5 Поддържана 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 се съхраняват за по-дълги периоди от време, доколкото личните данни 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 ГДРП, за да се защитят правата и свободите на субекта на данните.

2.6. Обработени 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. Правата на субектите на данни

GDPR определя следните права, приложими за субектите на данните (моля, направете справка в посочените в тази политика части за повече подробности):

3.1 Правото на информация (Част 12).

3.2 Правото на достъп (част 13);

3.3 Право на поправка (Част 14);

3.4 Правото за заличаване (известно също като "правото да бъде забравено") (част 15);

3.5 Право на ограничаване на обработката (Част 16);

3.6 Право на преносимост на данни (Част 17);

3.7 Право на възражение (Част 18); и

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

4. Законна, справедлива и прозрачна обработка на данни

4.1 GDPR се стреми да гарантира, че личните данни се обработват законно, 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 обработката на личните им данни за една или повече конкретни цели;

4.1.2 Обработката е необходима за изпълнение на договор, по който лицето, за което се отнасят данните, е страна или за да предприеме стъпки по искане на субекта на данните преди да сключи договор с тях;

4.1.3 Обработката е необходима за спазване на правно задължение, на което се подчинява администраторът на данните;

4.1.4 Обработката е необходима за защита на жизненоважните интереси на субекта на данните или на друго физическо лице;

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

4.1.6 Обработката е необходима за целите на легитимните интереси, преследвани от администратора на данни или от 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 Ако въпросните лични данни са "данни от специална категория" (известни също като "чувствителни лични данни" (например данни за расата, етническата принадлежност, политиката, религията, членството в синдикални организации, генетиката, биометричните

данни Идентификационни цели), здраве, сексуален живот или сексуална ориентация), трябва да бъде изпълнено поне едно от следните условия:

4.2.1 Субектът на данни е дал своето изрично съгласие за обработката на тези данни за една или повече конкретни цели (освен ако законодателството на ЕС или на държавите-членки на ЕС ги забранява да го направят);

4.2.2 Обработката е необходима за изпълнение на задълженията и упражняване на специфични права на администратора на данни 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 Обработката е необходима 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 обработката се осъществява в хода на легитимните й 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 Обработката се отнася до лични данни, които ясно се оповестяват от субекта на данните;

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

4.2.7 Обработката е необходима поради значими съображения от 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 Преработката е необходима за целите на превантивната или професионалната медицина, за оценяване на работоспособността на служител, 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 Обработката е необходима 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); или

4.2.10 Обработката е необходима за целите на архивирането в интерес на обществото, научните или историческите изследвания или статистическите в съответствие с член 89, параграф 1 от **Регламент (ЕС) 2016/679**, 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 субектите на данни за работниците и служителите, клиенти и доставчици.

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 тези Политика (или за други цели, изрично разрешени от GDPR).

5.3 Данните за служителите се информират по всяко време за целта или целите, за които дружеството използва личните им данни. Моля, вижте част 12 за повече информация относно информирането на субектите на данни.

6. Адекватна, подходяща и ограничена обработка на данни

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

7. Точност на данните и поддържане на данните актуални

7.1 Дружеството трябва да гарантира, че всички лични данни, събрани, обработени и съхранявани от него, се съхраняват точни и актуални. Това включва, но не се ограничава до поправянето на лични данни по искане на субект на данни на служител, както е посочено в част 14 по-долу.

7.2 Точността на личните данни се проверява, когато се събира и след това. Ако се установи, че лични данни са неточни или не са актуални, незабавно ще бъдат предприети 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 светлината на целта или целите, за които тези лични данни са били първоначално събрани, държани и обработени.

8.2 Когато личните данни вече не се изискват, всички разумни стъпки ще бъдат предприети, за да бъдат изтрити или по друг начин да бъдат унищожени незабавно.

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

9. Защитена обработка

Дружеството трябва да гарантира, че всички събрани, съхранявани и обработени лични данни са безопасни и защитени от неразрешена или незаконна обработка и от случайна загуба, унищожаване или повреда. Допълнителни подробности за техническите и организационни мерки, които трябва да бъдат предприети, са дадени в Части от 26 до 31 от настоящата Политика.

10. Отчетност и водене на записи

10.1 Служителят за защита на данните на фирмата е Николай Генчев, гр. Казанлък, ул. „Розова долина“ 100, П.К. 6100, тел: +359 431 6 33 22 ; факс: +359 431 6 33 32, имейл: arsenal@arsenal-bg.com.

10.2 Отговорникът по защита на данните е отговорен за надзор на изпълнението на тази Политика и за мониторинг на спазването на тази Политика, другите политики на компанията в областта на заетостта и защитата на данните, както и с GDPR и други приложими закони за защита на данните.

10.3 Дружеството трябва да води писмени вътрешни записи за събирането, съхраняването и обработката на лични данни, които включват следната информация:

10.3.1 Името и подробностите на компанията, нейния служител по защита на данните 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. Подробности за категориите на личните данни, събрани, съхранявани и обработвани от Дружеството, и категориите данни за служителите, за които се отнасят тези лични данни;

10.3.4 Подробности за всички прехвърляния на лични данни към страни извън ЕИП, включително всички механизми и предпазни мерки за сигурност;

10.3.5 Подробности за продължителността на съхраняването на лични данни от Компанията и

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

11. Оценки на въздействието върху защитата на данните

11.1 Дружеството ще извършва оценки 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 служители на данни за работниците и служителите съгласно GDPR].

11.2 Оценките на въздействието върху защитата на данните се контролират от служителя по защита на данните и се отнасят до следното:

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 за служителите;

11.2.8 Рискове, породени както от компанията, така и от нея; и

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 на служителя:

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

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

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

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

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 неговия служител по 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 обработка;

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

12.2.4 Когато личните данни не се получават директно от субекта на данните на 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 (вж. Част 32 от тази политика за допълнителни подробности);

12.2.7 Подробности за запазването на данни;

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

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

12.2.10 Подробности за правото на субекта на данните на служителите да подават жалби в Службата на комисаря по информацията ("надзорният орган" по Регламент (ЕС) 2016/679);

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

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 компанията 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 служителя за защита на данните на компанията, както следва: до Николай Генчев, гр. Казанлък, ул. „Розова долина“ 100, П.К. 6100, тел: +359 431 6 33 22 ; факс: +359 431 6 33 32, имейл: arsenal@arsenal-bg.com.

13.3 Отговорите обикновено се правят 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 на служителя трябва да бъде информиран.

13.4 Всички получени формуляри за заявка за достъп до данни се обработват от служителя на компанията 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 на служител 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 за работниците и служителите имат право да изискват от дружеството да коригира всякакви лични данни, които са неточни или непълни.

14.2 Компанията следва да поправи 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 на служителя 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, която трябва да бъде направена на тези лични данни.

15. Изтриване на лични данни

15.1 Субектите на данни имат право да поискат от Компанията 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 притежаването и обработката на личните им данни от дружеството;

15.1.3 Субектът на данни възразява срещу това, че Дружеството притежава и обработва личните им данни (и няма преимуществен законен интерес, за да позволи на Дружеството да продължи това) (вижте Част 18 от тези Политика за повече подробности относно правото на възражение) ;

15.1.4 личните данни са били обработени незаконно;

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

15.1.6 Личните данни се съхраняват и обработват с цел предоставяне на услуги на информационното общество на детето.

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

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

16. Ограничаване на обработката на лични данни

16.1 Субектите на данни за персонала могат да поискат Дружеството да прекрати обработването на личните данни, които притежава за тях. Ако даден субект на данни на служител направи 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 за работниците и служителите дадоха своето съгласие на Дружеството да обработва личните си данни по такъв начин, или обработката е иначе необходима за изпълнението на договор между Компанията и субекта на данни на служителя, субектите на данни за служителите имат право, под GDPR, да получават копие от личните им данни и да ги използват за други цели (а именно да ги предават на други администратори на данни).

17.3 За да се улесни правото на преносимост на данните, Дружеството трябва да предостави всички приложими лични данни на субектите на данни за служителите в следния формат (и):

17.4 Когато това е технически осъществимо, при поискване от субект на данни на служител, личните данни се изпращат директно до изисквания 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 на служителя. 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 на служителя трябва да бъде информиран.]

18. Възражения срещу обработката на лични данни

18.1 Субектите на данни за служителите имат право да възразят срещу това, че Дружеството обработва своите лични данни въз основа на законни интереси, директен маркетинг (включително профилиране), [и обработка за научни и / или исторически изследвания и статистически цели].

18.2 Когато даден субект на данни на служител 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 му данни за целите на директния маркетинг, Дружеството незабавно прекратява такава обработка.

18.4 Когато даден субект на данни за работника или служителя възразява срещу това, че Дружеството обработва личните си данни за научни и / или исторически проучвания и статистически цели, субектът на данни за работниците и служителите 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. << Вмъкване на подробности за автоматизираното вземане на решения >>.

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

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 на служителя;

19.3.2 Решението е разрешено от закона; или

19.3.3 Субектът на данните на служителите 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 на служителите, 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; и

20.2.4 Всички лични данни, обработвани за целите на профилирането, трябва да бъдат обезпечени, за да се предотвратят дискриминационни ефекти, произтичащи от профилиране (вж. 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 на служителите 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 име;

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 Етнически;

21.2.4 Националност;

21.2.5 Религия;

21.3 Здравни досиета (Моля, вижте 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 (където е приложимо) [(моля, вижте част 24, по-долу, за допълнителна информация)];

21.4.6 Информация за мониторинг на служителите (моля, вижте 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 [всички] субекти на данни за служителите, които се използват за оценка на здравето, благосъстоянието и благосъстоянието на служителите и за изясняване на всички въпроси, които могат да изискват по-нататъшно разследване. По-специално, компанията 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 дефиницията на GDPR за специални категории данни (вж. Част 4 от настоящата Политика за определение). Поради това всички данни, свързани със здравето на субектите на данните на служителите, 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 лице на физически лица.

22.2 Здравните досиета са достъпни и използвани само от служба „Трудова медицина“ към „АРСЕНАЛ“ АД 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 работника или служителя, на които се отнасят тези данни], освен в изключителни случаи, когато благосъстоянието на субекта на данните на работника или служителя, 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 за служителите имат право да поискат от компанията да не води здравни досиета за тях. Всички такива искания трябва да бъдат изпратени в писмен вид и адресирани до Николай Генчев – служител по защита на личните данни, email:

arsenal@arsenal-bg.com ; адрес: гр. Казанлък, ул. „Розова долина“ 100, П.К. 6100, тел: +359 431 6 33 22 ; факс: +359 431 6 33 32.

23. Ползи

23.1 В случаите, когато субектите на данни за работниците и служителите 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 за служителите.

23.2 Преди събирането на такива данни субектите на данни за работниците и служителите 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 е така необходими за администрирането на съответните схеми за обезщетения.

24. Синдикати

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

24.1.1 име;

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 за работниците и служителите имат правото 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 от време на време да наблюдава дейностите на субектите на данни за служителите. 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 за служителите ще бъдат информирани за точния характер на мониторинга в 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 за работниците и служителите задължения по Регламента.

25.4 Дружеството трябва да гарантира, че няма ли ненужно навлизане на личните комуникации или дейности на субектите на данни на служителите 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 ("ВЧМ"), предоставяна от компанията 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 тялото на 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 на лични данни 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 "поверителна".

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), дали такова устройство

принадлежи на Компанията или по друг начин без официално писмено одобрение на съответния ръководител на отдела 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; и

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 служителят по защита на данните - Николай Генчев, гр. Казанлък, ул. „Розова долина“ 100, П.К. 6100, тел: +359 431 6 33 22 ; факс: +359 431 6 33 32, имейл: arsenal@arsenal-bg.com.

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 служителят по защита на данните - Николай Генчев, гр. Казанлък, ул. „Розова долина“ 100, П.К. 6100, тел: +359 431 6 33 22 ; факс: +359 431 6 33 32, имейл: arsenal@arsenal-bg.com.

29.3 Личните данни трябва да се обработват с грижата по всяко време и не трябва да бъдат оставени без надзор или по преценка на неразрешени служители, агенти, подизпълнители или други страни по всяко време;

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; и

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 обработката 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 и им се предоставя копие от 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; и

31.11 Когато някой агент, изпълнител или друга страна, работеща 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. Прехвърляне на лични данни в страна извън ЕИП

32.1 Дружеството може от време на време да прехвърля ("прехвърляне" включва предоставяне на дистанционно) лични данни на страни извън ЕИП.

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

32.2.1 Прехвърлянето 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 Прехвърлянето 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 (например Службата на комисаря по информацията); 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 Прехвърлянето се извършва с информирано съгласие на съответния (ите) субект (и) на данните за служителите;

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

32.2.5 Прехвърлянето е необходимо поради важни причини от обществен интерес;

32.2.6 Прехвърлянето е необходимо за извършване на съдебни искове;

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

32.2.8 Прехвърлянето се извършва от регистър, който според законодателството на Обединеното кралство или ЕС е предназначен 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 легитимен интерес достъп до регистъра.

33. Уведомяване за нарушаване на данните

33.1 Всички нарушения на лични данни трябва да бъдат съобщени незабавно на дружеството Служител по 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 за служителите (напр. Финансови загуби, нарушаване на поверителността, дискриминация, репутационни щети или други значителни социални или икономически щети), Служителят по защита на данните трябва да гарантира, че Службата на комисаря по информацията е информирана незабавно за нарушението и при всички случаи в рамките на 72 часа след като е узнала 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 за служителите, служителят по защита на данните трябва да гарантира, че всички засегнати субектите на данни за служителите 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 служителя на компанията 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 в сила от 23.05.2018 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 проверена и одобрена от:

Име: Николай Христов Ибушев

Позиция: Изпълнителен директор

Дата: 23.05.2018 г.