

ВЪТРЕШНИ ПРАВИЛА

за защита на личните данни на физически лица, обработвани от БСК

Съдържание

Раздел 1. ОБЩИ ПОЛОЖЕНИЯ	2
1.1. Цели	2
1.2. Публичност	2
1.3. Обхват (средства за обработване)	2
1.4. Принципи на обработване	2
Раздел 2. ДЕЙНОСТИ ПО ОБРАБОТВАНЕ	3
2.1. Основания за обработване	3
2.2. Регистри с лични данни	4
2.3. Категории лични данни	4
2.4. Категории лица	4
2.5. Цели на дейностите по обработването	5
2.6. Пренос на данни	5
2.7. Срок на съхранение	6
Раздел 3. ПРАВА НА СУБЕКТИТЕ НА ДАННИ	6
3.1. Право на информация	6
3.2. Право на поверителност на данните	7
3.3. Право на достъп	7
3.4. Право да иска коригиране на обработването	8
3.5. Право на възражение срещу обработването	8
3.6. Право да иска ограничаване на обработването	8
3.7. Право на изтриване (правото да бъдеш забравен)	8
3.8. Право да изисква да не е обект на автоматизирано взети решения и автоматизирано профилиране	9
3.9. Право на преносимост на данните	9
3.10. Право на жалба	9
Раздел 4. МЕРКИ ЗА СИГУРНОСТ	9
4.1. Организационни мерки	9
4.2. Технически мерки	10
4.3. Унищожаване на лични данни	11
ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ	12
ПРИЛОЖЕНИЯ	14

Раздел 1. ОБЩИ ПОЛОЖЕНИЯ

1.1. Цели

1.1.1. Вътрешните правила имат за цел да осигурят защита на правата на физическите лица във връзка с обработването на лични данни от БСК, в качеството ѝ на администратор и обработващ лични данни (наричана по-нататък в правилата „администратор“), в съответствие с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. (Регламента) и разпоредбите на националното законодателство в областта на защитата на лични данни на физическите лица.

1.1.2. Вътрешните правила регламентират механизмите за водене на регистрите с лични данни в БСК, задълженията на длъжностните лица, обработващи лични данни и необходимите технически, и организационни мерки за защита на личните данни.

1.1.3. Вътрешните правила се прилагат от всички служители и всички изпълнители, които работят от името на администратора.

1.1.4. Вътрешните правила се прилагат за всички системи и процеси, които изграждат информационната система на администратора, съдържаща лични данни.

1.2. Публичност

1.2.1. Вътрешните правила за защита на личните данни са публично достъпни на сайта на БСК - www.bia-bg.com

1.2.2. Всяка актуализация на Вътрешните правила се извършва при посочване на датата на изменението и запазване на предходните версии по начин, който позволява тяхната проследимост на сайта на БСК.

1.3. Обхват (средства за обработване)

1.3.1. Вътрешните правила се прилагат за обработването на лични данни с технически средства и на хартиен носител.

1.4. Принципи на обработване

1.4.1. Обработването на личните данни се извършва при спазване на принципите на законосъобразност, добросъвестност, прозрачност, ограничение на целите, свеждане на данните до минимум, точност, ограничение на съхранението, сигурност, цялостност, поверителност и отчетност.

1.4.2. Администраторът спазва принципът на законосъобразност, като обработва лични данни на основание: съгласие на субекта; изпълнение на договор между субекта и администратора или предприемане на стъпки по искане на субекта на данните преди сключването на договор; спазването на законово задължение, което се прилага спрямо администратора; защита интересите на субекта; упражняване на официални правомощия, предоставени на администратора; законно основание.

1.4.3. Администраторът спазва принципът на добросъвестност, като преди обработването предоставя необходимата информация на субекта на данните, предвидена в Регламента, Закона за защита на личните данни и тези Вътрешните правила.

1.4.4. Администраторът спазва принципът на прозрачност, като осигурява достъп на субекта на данните, до неговите лични данни.

1.4.5. Администраторът спазва принципът на ограничение на целите, като събира личните данни за конкретни, изрично указани и легитимни цели и не обработва данните по начин, несъвместим с тези цели.

1.4.6. Администраторът спазва принципът на свеждане на данните до минимум, като събира лични данни, които са ограничени до минимално необходимото, за целите за които се обработват.

1.4.7. Администраторът спазва принципът на точност, като поддържа данните в актуален вид и предприема всички разумни мерки за своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват.

1.4.8. Администраторът спазва принципът на ограничение на съхранението, като съхранява личните данни във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни.

1.4.9. Администраторът спазва принципът на цялостност и поверителност, като прилага подходящи технически и/или организационни мерки, и обработва личните данни по начин, който гарантира

подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане.

1.4.10. Администраторът спазва принципът на отчетност, като е в състояние да докаже спазването на всички гореизброени принципи при обработването на лични данни и при въвеждането на нови средства и нови информационни системи за обработване.

Раздел 2. ДЕЙНОСТИ ПО ОБРАБОТВАНЕ

2.1. Основания за обработване

2.1.1. Правните основания за обработване на лични данни са:

- а/ законово задължение за администратора;
- б/ договор/предоговорни отношения;
- в/ изпълнение на задача от обществен интерес или упражняването на официални правомощия, предоставени на администратора;
- г/ за целите на легитимните интереси на администратора;
- д/ съгласие на субекта на данни.

2.1.2. (1) Преди да започне обработването, администраторът в достъпна форма и на ясен език информира субекта на лични данни относно правата му по отношение на неговите данни и за своите задължения при обработване на данните. ([Приложение 1](#))

(2) Заедно с информацията по ал. 1 администраторът запознава субекта на лични данни със задължението на субекта за опазване на професионална тайна и спазването на поверителност при обработването на данните, ако е приложимо.

(3) Когато обработването е на основание съгласие, администраторът информира субекта за правата му по ал. 1, както и правото да посочи целите на обработването и правото да оттегли съгласието си.

2.1.3. Съгласието трябва да е:

- а/ свободно изразено – в резултат на свободната воля на субекта, а не под натиск или заплаха;
- б/ конкретно – съдържа конкретната цел на обработването;
- в/ информирано – дадено на основата на познаване на настоящите правила и при необходимост по искане на субекта – на допълнителни разяснения към тях;
- г/ изрично заявено.

2.1.4. Съгласието се изразява в изрична писмена декларация, в която субектът посочва конкретната цел/и на обработването и че е запознат с правата си по отношение на личните си данни, включително с правото да оттегли съгласието си. ([Приложение 2](#) и [Приложение 3](#))

2.1.5. Счита се че има изрично съгласие, при писмено изявление инкорпорирано в друг документ (договор, заявление, молба и др.), в които се посочват целите на обработването и обстоятелството, че субектът е запознат с правата си по отношение на неговите лични данни, включително правото да оттегли съгласието си.

2.1.6. Съгласието на дете при навършена 16-годишна възраст се изразява по реда на т.2.1.4. и т. 2.1.5.

2.1.7. Съгласието на дете при ненавършена 16-годишна възраст се изразява от лицето упражняващо родителски права или настойника, по реда на т. 2.1.4. и т. 2.1.5. ([Приложение 4](#))

2.1.8. Субектът на данни има право да бъде информиран и да даде допълнително съгласие, ако е необходимо по-нататъшно обработване на данните за цели, различни от първоначално посочените.

2.1.9. Оттеглянето на съгласието се извършва в изрична писмена форма. ([Приложение 5](#))

2.1.10. Администраторът е отговорен за опазване на съгласието и на оттеглянето на съгласието на субекта на данни. ([Приложение 6](#) и [Приложение 7](#))

2.2. Регистри с лични данни

2.2.1. Настоящите вътрешни правила се отнасят за обработването на лични данни в следните регистри, водени на функционален принцип в БСК:

- а/ регистър на лични данни по трудови правоотношения;
- б/ регистър на лични данни по граждански договори с изпълнители;
- в/ регистър лични данни на органи на управление и контрол на БСК;
- г/ регистър на лични данни на Националния съвет на председателите;
- д/ регистър на лични данни на лица, които управляват и/или представляват членове на БСК;
- е/ регистър на лични данни на местни органи на БСК, по смисъла на чл. 35 ал. 1 т. 3 от КТ;
- ж/ регистър на лични данни на лица, които управляват и/или представляват български и чуждестранни партньори на БСК;
- з/ регистър на лични данни на лица, представляващи и/или управляващи търговски партньори на БСК;
- и/ регистър на лични данни на лица, управляващи и/или представляващи сдружения, в които БСК членува, или търговски дружества, в които БСК има дялово или акционерно участие;
- й/ регистри на лични данни на обучаеми лица и лица, участващи в срещи, семинари, конференции и др. форуми, организирани от БСК;
- к/ регистри на лични данни на членове на секторни консултативни съвети и други временно функциониращи структурни звена;
- л/ регистри на лица, свързани с издаването на сертификати за произход на стоките;
- м/ регистри на лица, свързани с издаването на сертификати за форсмажор;
- н/ регистри на субекти на данни, които се събират във връзка с функционирането на Арбитражния съд при БСК;
- о/ регистри на данни, събирани при използване на информационни технологии;
- п/ регистър на представители на средствата за масова информация.

2.3. Категории лични данни

2.3.1. Обикновени категории данни, които се обработват от администратора са: имена, единен граждански номер, данни по документи за самоличност, временен и постоянен адрес, имейл адрес, месторождение, телефони за връзка, възраст, данни за образование, квалификация, трудов стаж, професионална биография, данни за семейно положение и деца под 18 години (ако е необходимо за упражняване на трудови и свързани с тях права), данни относно доходи по трудови и граждански отношения - предоставят се на основание нормативно задължение за изпълнение на съответни задължения към данъчни и осигурителни органи или въз основа на съгласие на субектите на данни.

2.3.2. Специалните категории данни, които се обработват от администратора, са:

- а/ които се събират по силата на закон, относно здравен статус (данни за физиологичното, психическо и психологическо състояние на физическото лице - данните са от значение при заемане на длъжности и изпълнение на функции, изискващи особено висока степен на отговорност, заключение на лекарска комисия, информация от служба по трудова медицина), доколкото са необходими за защита правата на субекта на данните при осъществяване на трудовите и свързаните с тях отношения; за превантивна или трудова медицина, за оценка на трудоспособността;
- б/ които се събират по силата на закон относно наказателноправен статус - свидетелство за съдимост, удостоверение, че лицето не е под съд и следствие (ако е приложимо за заемане на длъжност или изпълняване на конкретна дейност).

2.4. Категории лица

2.4.1. Категориите лица, от които се събират лични данни, са:

- а/ работници и служители;
- б/ изпълнители по граждански договори;

- в/ партньори по търговски договори, договори по изпълнение на проекти с европейско и международно финансиране;
- г/ лица, които представляват членове на БСК;
- д/ членове на управителни и контролни органи на БСК;
- е/ лица, представляващи организации, в които БСК е партньор или член;
- ж/ лица, представляващи местни органи на БСК по смисъла на КТ;
- з/ арбитри в Арбитражния съд към БСК;
- и/ лица, които представляват страни по арбитражни дела в Арбитражния съд към БСК;
- й/ вещи лица и свидетели по дела в Арбитражния съд към БСК;
- к/ участници в обучения, семинари, анкетни проучвания, конференции, форуми и др. събития, организирани от БСК;
- л/ лица, кандидатстващи за работа;
- м/ лица, участващи в търгове и конкурси;
- н/ представители на средствата за масова информация;
- о/ данни за непълнолетни лица – по искане на родител, който е свързан с БСК по силата на трудови правоотношения.

2.5. Цели на дейностите по обработването

2.5.1. Използване на личните данни за съответните служебни цели - възникване, изменение и прекратяване на трудови, граждански отношения или функции, които се упражняват по силата на закон или устава на организацията; за водене на счетоводна отчетност относно възнаграденията; за установяване на връзка с лицата по телефон, имейл, домашен адрес и за изпращане на кореспонденция, свързани със служебни, уставни, членствени, управленски и др. отношения; за изпращане на информация; изработване на документи, свързани с тези отношения; за обработка на плащания по сключени договори; извършване на проучвания, провеждане на обучения, изпълнение на проекти и обществени поръчки; защита на законни права на субектите на данни, защита на интересите на администратора на данни.

2.5.2. Администраторът гарантира, че при дадено съгласие на субекта на данни, обработването се извършва само за целите, посочени изрично в съгласието.

2.5.3. Администраторът гарантира, че при необходимост от обработване на данните за цел различна от първоначалната ще информира субекта на данни и при необходимост ще изиска съгласието му.

2.6. Пренос на данни

2.6.1. (1) Получатели на личните данни, обработвани от администратора по силата на законови разпоредби, са:

- а/ по трудови отношения – Националната агенция по приходите, Националният осигурителен институт, ИА Главна инспекция по труда, Службата по трудова медицина;
- б/ по членствени правоотношения и управителни и контролни органи – Министерският съвет, Министерството на труда и социалната политика, Агенцията по вписванията, съд;
- в/ по арбитражни дела – съд, съдебни изпълнители;
- г/ по сертификати за произход на стоките - митнически органи в страната и в чужбина, Министерство на финансите;
- д/ други публични органи, които получават данните по силата на закон.

(2) За целите на легитимните интереси на администратора на лични данни – на органи и организации в страната и в чужбина - за целите на участия в срещи, работни групи, конференции, комитети, комисии и др., свързани с дейността на БСК, както и при изпълнение на проекти и обществени поръчки.

(3) На основание съгласие на работника или служителя – информация на сайта на БСК, свързана със субекта на данни.

2.6.2. Администраторът се задължава предаването на лични данни на трета държава или на международна организация да се осъществява само при условие, че са спазени разпоредбите на Регламента, включително във връзка с последващи предавания на лични данни от третата държава или от международната организация на друга трета държава или на друга международна организация, за да се осигури необходимото ниво на защита на физическите лица.

2.7. Срок на съхранение

2.7.1. Сроковете на съхранение на данните са:

- а/ Законоустановени срокове за съхранение на данни по трудови правоотношения, вкл. ведомости за заплати – 50 години, счетоводни регистри - 10 години, считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят;
- б/ Срокове, свързани с преклудирането на права по законоустановени давностни срокове, свързани със задължения по граждански и търговски договори – 3 години за периодични плащания и 5 години в останалите случаи, считано от датата на изискуемостта на вземането;
- в/ Срокове, свързани с целите на обработване – договорни срокове, срокове по приключване и отчитане на договорни и финансови отношения по договори, свързани с национално, европейско и международно финансиране – срокове, посочени в договори или общи условия, и срокове, свързани с преклудиране на права;
- г/ Срокове, свързани с информация за целите на данъчно и счетоводно отчитане, данъчни проверки и ревизии и държавен финансов контрол;
- д/ Срокове свързани с получаване на информационни и други бюлетини от електронната страница на БСК и други изнформационни системи, администрирани от БСК, въз основа на съгласие на субекта на данни – до оттегляне на съгласието, респ. прекратяване на акаунт/регистрация;
- е/ Данни, събирани при използване на информационни технологии – Адрес на интернет протокол (IP), Идентификационен номер на „бисквитка“ – 3 месеца;
- ж/ Интернет трафик на персонални компютри – 1 седмица;
- з/ Логове, свързани със сигурност, техническа поддръжка, развитие и др. - 3 месеца;
- и/ Съвързни логове, логове на устройства за защита на сигурността (Web Application Firewalls) и др. устройства, попадащи в тази категория - 3 месеца;
- й/ Регистри на данни, събирани при видеонаблюдение – 1 седмица;
- к/ Данни за оттеглено съгласие от субекта на данни – безсрочно;
- л/ Данни на кандидати за заемане на длъжности при администратора - 30-дневен.

2.7.2. След изтичане на сроковете за съхранение данните на технически носител се заличават, а на хартиен – ако не подлежат на предаване за съхранение по закон, се унищожават.

Раздел 3. ПРАВА НА СУБЕКТИТЕ НА ДАННИ

3.1. Право на информация

3.1.1. Субектът на данни има право на информация относно:

- а/ данни, които идентифицират администратора – наименование, контактни данни на администратора и посочени от него длъжностни лица;
- б/ цели и правно основание на обработването;
- в/ (категории) получатели на личните му данни;
- г/ условия за трансфер на личните данни, вкл. на трета държава или международна организация;
- д/ срок за съхранение на данните и/или критерии за определяне на срока;
- е/ извършване на видеонаблюдение на работното място;

ж/ следене от работодателя на средствата за електронна комуникация на работното място, предоставени от дружеството/организацията (интернет, телефон, мобилен телефон) с цел предотвратяване на злоупотреби.

з/ информация за източника на данни, когато е различен от субекта на данни.

3.1.2. Настоящите правила и информацията за поверителност на администратора се публикува на интернет страницата на администратора, с цел субектите на данни, за които не е относимо подписването на информацията за поверителност, да бъдат информирани за правата си и условията за събиране и обработване на данни.

3.2. Право на поверителност на данните

3.2.1. Личните данни остават поверителни при спазване на задължение за опазване на професионална тайна, за което служителите на БСК са информирани с подписване на декларация за поверителност. ([Приложение 8](#))

3.3. Право на достъп

3.3.1. Субектът на данните има право да получи от администратора потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните и следната информация:

- а) целите на обработването;
- б) съответните категории лични данни;
- в) получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;
- г) когато е възможно, предвиденият срок, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определянето на този срок;
- д) съществуването на право да се изиска от администратора коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или да се направи възражение срещу такова обработване;
- е) правото на жалба до надзорен орган;
- ж) когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник;
- з) съществуването на автоматизирано вземане на решения, включително профилиране.

3.3.2. Субектът на данни има право да получи копие от личните данни, които са в процес на обработване в електронна форма или на хартиен носител.

3.3.3. Субектът на лични данни подава писмено заявление лично или чрез упълномощено лице до обработващия лични данни, в т. ч. по електронен път.

3.3.4. Подаването на заявление и еднократното предоставяне на лични данни е безплатно. Администраторът предоставя копие от личните данни, които са в процес на обработване. За допълнителни копия, поискани от субекта на данните, администраторът може да наложи разумна цена въз основа на административните разходи.

3.3.5. Заявлението съдържа име на лицето, единен граждански номер, описание на искането, предпочитана форма за предоставяне достъпа до лични данни, подпис, дата и адрес за кореспонденция. Към заявлението се прилага пълномощно, когато се подава от упълномощено лице. Заявлението се завежда във входящ регистър на администратора на лични данни. ([Приложение 9](#))

3.3.6. Достъпът до данните на лицето се осигурява под формата на:

- а/ устна справка;
- б/ писмена справка;
- в/ преглед на данните от субектът на данните или упълномощено от него лице;
- г/ предоставяне на копие от исканата информация;
- д/ предоставяне на исканата информация по електронен път, освен в случаите, когато това е технически невъзможно или забранено от закон.

3.3.7. Срокът за разглеждане на заявлението и произнасяне по него е 14-дневен от деня на подаване на искането и може да бъде удължен до 30-дневен, когато е необходимо повече време за събиране на личните данни на лицето, с оглед възможни затруднения в дейността на администратора.

3.3.8. Решението се съобщава писмено на заявителя лично срещу подпис или по пощата с обратна разписка. Когато данните не съществуват или не могат да бъдат предоставени на определено правно основание, на заявителя се отказва достъп до тях с мотивирано решение. Отказът за предоставяне достъп може се обжалва от лицето пред посочения в писмото орган и срок.

3.4. Право да иска коригиране на обработването

3.4.1. Субектът на данни има право да поиска от администратора да коригира и допълни без ненужно забавяне неточните лични данни, свързани с него.

3.5. Право на възражение срещу обработването

3.5.1. Субектът на данни има право на възражение срещу обработването, когато обработването не е основано на императивни разпоредби на законодателството.

3.5.2. Субектът на данни има право по всяко време да направи възражение срещу обработване на личните му данни за целите на директния маркетинг.

3.6. Право да иска ограничаване на обработването

3.6.1. Субектът има право да поиска ограничаване на обработването в следните случаи:

- а/ точността на личните данни се оспорва от субекта на данните за срок, който позволява на администратора да провери точността им;
- б/ обработването е неправомерно;
- в/ след отпадане на необходимостта от обработване на личните данни от администратора, субектът ги изисква с цел установяването, упражняването или защитата на правни претенции;
- г/ след възражение на субекта на данни срещу обработването;
- д/ очакване на проверка дали законните основания на администратора имат преимущество пред субекта на данните.

3.6.2. Искането се осъществява с писмена молба.

3.6.3. Когато обработването на данни е ограничено по реда на т. 3.6.1., данните се съхраняват от администратора и обработват само със съгласието на субекта на данните или за установяването, упражняването или защитата на правни претенции, или за защита правата на друго физическо лице, или поради важни основания от обществен интерес, за ЕС или държавите-членки.

3.6.4. Когато субект на данните е изискал ограничаване на обработването на данни, администраторът го уведомява преди отмяната на ограничаване на обработването.

3.7. Право на изтриване (правото да бъдеш забравен)

3.7.1. Субектът може да поиска данните му да бъдат изтрити, а администраторът е задължен да ги изтрие без забавяне, ако:

- а/ не са му необходими за целите, за които са били събирани или обработвани;
- б/ ако субектът оттегли съгласието си за обработване на данните и няма друго основание за обработване;
- в/ субектът на данните възразява срещу обработването и няма законни основания за обработването или субектът на данните възразява срещу обработването, когато се обработват за целите на директния маркетинг;
- г/ данните са били обработвани незаконосъобразно;
- д/ личните данни трябва да бъдат изтрити с цел спазване на законово задължение, произтичащо от националното законодателство или от правото на ЕС;
- е/ личните данни били са събирани за целите на информационното общество.

3.7.2. Искането за изтриване на данните не се удовлетворява, ако обработването е необходимо на законно основание или за упражняване на задача от обществен интерес, или за установяването, упражняването или защитата на правни претенции.

3.7.3. Администраторът разглежда исканията при спазване на процедура ([Приложение 10](#)) и съобщава на субекта на данни за всяко извършено коригиране, изтриване или ограничаване на обработването на всеки получател, на когото личните данни са били разкрити, освен ако това е невъзможно или изисква несъразмерно големи усилия. Администраторът информира субекта на данните относно тези получатели, ако субектът на данните поиска това.

3.8. Право да изисква да не е обект на автоматизирано взети решения и автоматизирано профилиране

3.8.1. Субектът на данни има право да изисква от администратора да не бъде обект на автоматизирано взети решения, които го засягат в значителна степен, без възможност за човешка намеса;

3.8.2. Субектът на данни има право да се противопостави на автоматизирано профилиране, когато не е дал съгласие за това.

3.9. Право на преносимост на данните

3.9.1. Субектът на данни има право да получи личните си данни, които го засягат и които той е предоставил на администратора, в структуриран, широко използван и пригоден за четене формат и има право да прехвърли тези данни на друг администратор без възпрепятстване от администратора, на когото личните данни са предоставени, когато обработването е основано на съгласие или на договорно задължение, при условие, че администраторът ги обработва по автоматизиран начин. ([Приложение 11](#))

3.10. Право на жалба

3.10.1. Субектът на данни има право на жалба до администратора ([Приложение 12](#)), по процедура ([Приложение 13](#)), относно:

- а/ обработването на лични данни;
- б/ обработване на искане на субекта на данни;
- в/ обработване на жалба от субекта на данни.

3.10.2. Субектът на данни има право на жалба до надзорен орган, ако някоя от разпоредбите за обработване на лични данни е нарушена.

3.10.3. Администраторът съдейства на субектите на данни за упражняването на техните права, като ги информира относно правата им и се стреми да удовлетвори исканията им.

3.10.4. Администраторът спазва срокове и процедури за разглеждане на исканията и уведомяване на Надзорния орган за нарушение на сигурността ([Приложение 14](#) и [Приложение 15](#)).

3.10.5. Администраторът е длъжен да разгледа всяко искане на субекта на данни, включително когато то е направено в свободна форма, а не по образците-приложения към тази Политика.

3.10.6. При необходимост администраторът оказва помощ на субекта на данни да оформи исканията си в подходяща форма.

3.10.7. Администраторът води дневник на исканията и жалбите на субектите на данни.

Раздел 4. МЕРКИ ЗА СИГУРНОСТ

4.1. Организационни мерки

4.1.1. За постигане на целите на настоящите Вътрешните правила и осигуряване сигурността на личните данни, администраторът предприема следните организационни мерки:

- а/ извършване на предварителен и текущ (ежегоден) анализ и оценка на риска по отношение на дейностите по обработване на данните;
- б/ определяне на служител, отговарящ за защита на данните;
- в/ обучение на персонала.

4.1.2. При извършване на анализ и оценка на риска се съобразява: извършва ли се обработване на „чувствителни“ данни; извършва ли се мащабно обработване на лични данни или мащабно наблюдение; брой на обработваните лични данни; осъществява ли се автоматично обработване, включително профилиране, които засягат субекта на данни; осъществява ли се псевдонимизация, криптиране, оценка на рисковете за правата и свободите на субектите на данни; мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни; оценка дали предложеното обработване на лични данни е едновременно необходимо и пропорционално за целите, за които се извършва; състоянието на техниката в организацията, цената на изпълнение по внедряване на нови технологии, ако се налагат такива, видовете обработване на лични данни и свързания риск за правата на субектите.

4.1.3. Степента на риска се определя от нивото на въздействие, което нарушаването на поверителността, цялостността или наличността на личните данни би оказало върху субекта/субектите на данни.

4.1.4. При идентифициран висок риск по отношение защитата на данните администраторът определя допълнителни адекватни технически и организационни мерки за защита на личните данни.

4.2. Технически мерки

4.2.1. Всички служители на администратора, които обработват лични данни, са отговорни за гарантирането на сигурността при съхраняването на данните, за които те отговарят, и се задължават да не разкриват тези данни на трети страни, освен ако администраторът не е дал такива права на тази трета страна по договорна клауза за поверителност.

4.2.2. Всички служители на администратора, които обработват лични данни:

- а/ са длъжни да познават и прилагат Политиката за защита на личните данни и настоящите правила;
- б/ съхраняват личните данни в затворени шкафове;
- в/ поддържат чисто работно място;
- г/ осигуряват контролиран достъп до работните си помещения;

4.2.3. Достъпът до информационните системи и цифрови носители се осъществява при спазване на следните правила:

- а/ достъпът до сървърите трябва да бъде оторизиран от Системния администратор;
- б/ системният администратор дефинира правата за достъп до съответните ресурси;
- в/ прегледът на правата за достъп се извършва от Системния администратор заедно с ИТ директора;
- г/ достъп до приложения софтуер и всяка друга информация имат само упълномощени потребители;
- д/ при работа с данните се използват софтуерни продукти, които са адаптирани към специфичните нужди на администратора на лични данни;
- е/ достъп до персонален компютър, съдържащ файлове за обработка на лични данни, има само обработващият и/или лицето, действащо под негово или на администратора ръководство;

4.2.4. Защитата на електронните данни от неправилен достъп, повреждане, изгубване или унищожаване, се осигурява посредством поддържане на софтуерни и хардуерни защити, антивирусни програми, периодично архивиране на данните.

4.2.5. Отнемането на правата на достъп се осъществява при спазване на следните правила:

- а/ при напускане на служител или прекратяване на договор с контрагент правата за достъп се отнемат от Системния администратор на база обходен лист или договор;
- б/ ако напускащият служител знае пароли за акаунти, които ще останат действащи, тези пароли трябва да бъдат сменени при неговото напускане или при промяна на работното място, договора или споразумението.

4.2.6. Използването на мрежовите услуги се осъществява при спазване на следните правила:

- а/ ползването на мрежовите услуги се управлява чрез персонален достъп до тях;

б/ потребителите имат достъп само до ресурсите и услугите, които са им необходими за реализиране на служебните им задължения.

4.2.7. Политиката на осъществяване на сигурност при влизане в системата се осъществява при спазване на следните правила:

а/ достъпът до информационните системи става чрез защитен процес на регистрация или оторизация с потребителско име и парола;

б/ неуспешните опити за регистрация или оторизация в системата се записват в логовете на съответната система;

в/ всички злонамерени опити за неоторизиран достъп до системите се анализират и регистрират в зависимост от нивото на заплахата.

4.2.8. Идентификация и автентификация на потребителя се осъществява при спазване на следните правила:

а/ всички потребители имат уникален идентификатор (ID) изключително за персонална употреба;

б/ този механизъм за контрол се прилага за всички потребители;

в/ потребителските идентификатори (user ID) се използват, за да се проследяват действията на отговорното лице. Обичайните дейности на потребителя не се извършват през привилегировани профили (акаунти).

г/ автентификацията на потребител се извършва чрез въвеждане на парола, която съответства на уникалния идентификатор на потребителя и е известна само на дадения потребител.

д/ право да използва системни програми има Системният администратор;

е/ на потребителите без администраторски привилегии е забранено използването на системни програми;

ж/ всички ненужни, обслужващи програми и системен софтуер биват премахвани или спирани.

4.2.9. Администраторът - Българска стопанска камара-съюз на българския бизнес, е оценена и сертифицирана съгласно изискванията на ISO/IEC 27001:2013.

4.3. Унищожаване на лични данни

4.3.1. Унищожаването на личните данни ([Приложение 16](#)) се извършва чрез:

а/ изтриване на информацията върху записващи носители;

б/ бракуване на записващи носители, за което се съставя протокол.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§1. Понятия:

„Лични данни“ - всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

„Специални категории лични данни“ – лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, или членство в синдикални организации и обработката на генетични данни, биометричните данни за уникално идентифициране на физическо лице, данни, отнасящи се до здравето, или данни относно сексуалния живот на физическо лице или сексуална ориентация.

„Обработване“ - означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбинирание, ограничаване, изтриване или унищожаване;

„Администратор“ – по смисъла на настоящата политика е Българска стопанска камара – съюз на българския бизнес.

„Субект на данните“ – всяко физическо лице, което е предмет на личните данни, съхранявани от Администратора.

„Съгласие на субекта на данните“ - всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

„Дете“ – всяко физическо лице на възраст под 16 години.

„Профилиране“ - всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно - за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение;

„Нарушение на сигурността на лични данни“ - нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

„Получател“ - физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна, или не. Същевременно, публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели“; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;

„Трета страна“ – всяко физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

„Ограничаване на обработването“ означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;

„Псевдонимизация“ означава обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни

мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано;

„Регистър с лични данни“ означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;

„Данни за здравословното състояние“ означава лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние;

„Надзорен орган“ означава независим публичен орган от държава членка на Европейския съюз, отговорен за наблюдението на прилагането на правилата за защита на личните данни, с които са въведени разпоредбите на Директива 2016/680 в съответното национално законодателство, с цел да се защитят основните права и свободи на физическите лица във връзка с обработването на лични данни и да се улесни свободното им движение в рамките на ЕС. За Република България надзорен орган е Комисията за защита на личните данни.

„Международна организация“ означава организация и нейните подчинени органи, регламентирани от международното публично право, или друг орган, създаден чрез или въз основа на споразумение между две или повече държави.

ПРИЛОЖЕНИЯ

Приложение 1

ИНФОРМАЦИЯ ОТНОСНО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ НА ФИЗИЧЕСКИ ЛИЦА ОТ СДРУЖЕНИЕ С НЕСТОПАНСКА ЦЕЛ БЪЛГАРСКА СТОПАНСКА КАМАРА – съюз на българския бизнес (БСК)

Данни за контакт с БСК:

Местоположение:

Държава: Република България

Адрес: София, община Столична, ул. „Алабин“ 16-20

Телефон: (02) 932 09

Ел. поща: office@bia-bg.com

Интернет страница: www.bia-bg.com

Данни за контакт с отговорник по защита на данните:

Ел. поща: office@bia-bg.com

Тел: (02) 932 09

Поверителност при обработката на лични данни:

БСК събира и обработва лични данни при спазване на принципа „свеждане на данните до минимум“, единствено и само за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели.

БСК прилага необходимите технически и организационни, с оглед осигуряване на поверителност и конфиденциалност на личните данни на физическите лица.

1. Категориите лични данни, които БСК обработва, са:

1.1. Обикновени категории данни:

а/ имена, единен граждански номер, дата и място на раждане, възраст, пол, гражданство, данни по документи за самоличност, данни за образование, квалификация, трудов стаж, професионална биография;

б/ данни за контакт - телефони за връзка , временен и постоянен адрес, имейл адрес;

в/ данни за семейно положение и деца под 18 години (ако е необходимо за защита правата на работник или служител);

г/ данни относно доходи по трудови и граждански отношения - предоставят се на нормативно основание изпълнение на задължения към данъчни и осигурителни органи.

1.2. Специални категории данни: които се събират по силата на нормативен акт относно здравен статус (данни относно физиологичното, психическо и психологическо състояние на физическото лице - данните са от значение при заемане на длъжности и изпълнение на функции, изискващи особено висока степен на отговорност, заключение на лекарска комисия, информация от служба по трудова медицина), доколкото са необходими за защита правата на субекта на данните при осъществяване на трудовите и свързаните с тях отношения; за извършване и стажуване; за превантивна или трудова медицина, за оценка трудоспособността;

1.3. които се събират по силата на нормативен акт относно наказателноправен статус - свидетелство за съдимост, удостоверение, че лицето не е под съд и следствие (ако е приложимо за заемане на длъжност или изпълняване на конкретна дейност).

1.4. БСК може да осъществява видеонаблюдение при спазване на ЗЧОД и ЗЗЛД.

2. Източник на личните данни, които БСК обработва, са:

2.1. субектът на данните;

2.2. публични регистри с лични данни, до които е осигурен свободен достъп;

2.3. документи, издадени от компетентни органи;

2.4. трети лица, във връзка или по повод на участието им в процедури за избор на изпълнител.

3. Личните данни, които БСК обработва, ще бъдат използвани единствено за следните цели:

3.1. подбор на персонал, възникване, изменение и прекратяване на трудови и свързани с тях отношения, които се упражняват по силата на закон; за водене на счетоводна отчетност относно възнагражденията, за данъчни и осигурителни цели; за установяване на връзка с лицата по телефон, имейл, домашен адрес и за изпращане на кореспонденция, свързани със служебни, уставни, членствени, управленски и др. отношения; изработване на документи, свързани с тези отношения; защита на законни права на субектите на данни; защита на интересите на администратора на данни;

3.2. за изпълнение на задължения по сключени договори; за упражняване на права, произтичащи от сключени договори; за целите на отчитане изпълнението на договори; одит на изпълнението на договори; за предприемане стъпки по искане субекта на данни преди сключване на договор;

3.3. за цели, изрично посочени в декларация-съгласие на субекта на данни за обработване на личните му данни;

3.4. за комуникация с информационна, рекламна и/или маркетингова цел, БСК ще поиска от вас допълнително съгласие.

3.5. БСК гарантира, че при дадено съгласие на субекта на данни, обработването се извършва само за целите, посочени изрично в съгласието.

3.6. БСК гарантира, че при необходимост от обработване на данните за цел, различна от първоначалната, ще информира субекта на данни и при необходимост, ще изиска съгласието му.

4. Основанието, което дава право на БСК да обработва вашите данни, е:

4.1. законово задължение за администратора;

4.2. изпълнение на договор/предоговорни отношения;

4.3. изпълнение на задача от обществен интерес или упражняването на официални правомощия, предоставени на администратора;

4.4. за защита на легитимните интереси на администратора или на субекта на данни;

4.5. съгласие на субекта на данни;

5. Легитимните интереси при обработването на данните, преследвани от БСК или от трети страни, които работят за БСК, са следните:

5.1. интереси, произтичащи по силата на закон за БСК, от качеството ѝ на работодател;

5.2. интереси, произтичащи по силата на закон за БСК, от качеството ѝ на представителна организация на работодателите на национално равнище;

5.3. интереси, произтичащи по силата на закон за БСК, от качеството ѝ на организация, защитаваща интересите на членовете си.

6.Последици от отказ от предоставяне на лични данни

6.1.Когато основанието за предоставяне и обработване на данни е съгласие или изпълнение на договор/предоговорни отношения, отказът на субекта от предоставяне на личните му данни има за последица невъзможност за установяване на отношения и/ или предоставяне на услуга и/или сключване на договор, с оглед на които са поискани данните.

7. БСК може да предаде личните Ви данни:

- 7.1. на законово основание – на държавни органи; на търговски дружества, сродни сдружения и други организации, във връзка с изпълнение на служебните Ви задължения;
- 7.2. на договорно основание – за заплащане на възнаграждения и за защита на интересите Ви по трудови и свързани с тях отношения;
- 7.3. на лица, на които по договор са възложени действия по водене на счетоводство;
- 7.4. на основата на Ваше съгласие – в съответствие със съгласието.

8. Съгласие

- 8.1. В случаите, когато БСК иска съгласие за специални (чувствителни) лични данни, ще обосновава необходимостта от тази информация и целите на обработването.
- 8.2. Имате право по всяко време с писмено изявление по образец или в свободна форма да оттеглите съгласието си за обработването на личните Ви данни от БСК.

9. Сроковете за съхранение на Вашите лични данни са:

- 9.1. законоустановени срокове за съхранение на данни - по трудови правоотношения, вкл. ведомости за заплати – 50 години, счетоводни регистри - 10 години, считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят;
- 9.2. срокове, свързани с преклудирането на права по законоустановени давностни срокове, свързани със задължения по граждански и търговски договори – 3 години за периодични плащания и 5 години в останалите случаи, считано от датата на изискуемостта на вземането;
- 9.3. срокове, свързани с целите на обработване – договорни срокове, срокове по приключване и отчитане на договорни и финансови отношения по договори, свързани с национално, европейско и международно финансиране – срокове, посочени в договори или общи условия, и срокове, свързани с преклудиране на права;
- 9.4. срокове, свързани с информация за целите на данъчно и счетоводно отчитане, данъчни проверки и ревизии и държавен финансов контрол.
- 9.5. данни, получени въз основа на съгласие на субекта на данни, за получаване на инфограционни и други бюлетини от електронната страница на БСК и други инфограционни системи, администрирани от БСК – до оттегляне на съгласието, респ. - прекратяване на акаунт/регистрация;
- 9.6. данни, събирани при използване на инфограционни технологии:
 - а/данни, събирани при използване на инфограционни технологии – Адрес на интернет протокол (IP), Идентификационен номер на „бисквитка“ – 3 месеца;
 - б/ интернет трафик на персонални компютри – 1 седмица;
 - в/ логове, свързани със сигурност, техническа поддръжка, развитие и др. - 3 месеца;
 - г/ сървърни логове, логове на устройства за защита на сигурността (Web Application Firewalls) и др. устройства, попадащи в тази категория - 3 месеца;
 - д/ данни за оттеглено съгласие от субекта на данни – безсрочно;
 - е/ данни на кандидати за заемане на длъжности при администратора - 30-дневен след приключване на процедурата за кандидатстване и подбор.
- 9.7. След изтичане на сроковете за съхранение, ако не е налице друго основание за обработването им, данните на технически носител ще бъдат заличени, а на хартиен – ако не подлежат на предаване за съхранение по закон, ще бъдат унищожени.

10. Вашите права като субект на личните данни са следните:

- 10.1. да поискате копие от Вашите лични данни от БСК и право на достъп по всяко време до личните си данни;
- 10.2. да поискате от БСК личните си данни във вид, удобен за прехвърляне на друг администратор на лични данни, или да поискате БСК да го направи, когато сте ни ги предоставили в структуриран, широко използван и пригоден за четене формат, когато обработването е основано на съгласие или на договорно задължение, при условие, че БСК ги обработва по автоматизиран начин;

10.3. да поискате от БСК да коригира без ненужно забавяне неточните Ви лични данни, както и данните, които не са вече актуални;

10.4. да поискате от БСК личните Ви данни да бъдат изтрети без ненужно забавяне при наличието на някое от следните основания:

- а/ личните данни повече не са необходими за целите, за които са били събрани;
- б/ когато сте оттеглили своето съгласие;
- в/ когато сте възразили срещу обработването;
- г/ когато обработването е незаконосъобразно;
- д/ когато личните данни трябва да бъдат изтрети с цел спазването на правно задължение по правото на ЕС или правото на държава-членка, което се прилага спрямо БСК като администратор на лични данни;
- е/ когато личните данни са били събрани във връзка с предлагането на услуги на информационното общество.

10.5. да поискате БСК да ограничи обработването на личните Ви данни. В този случай данните ще бъдат съхранявани, но не и обработвани, освен ако съществува законно основание за това;

10.6. да възразите срещу определени видове обработка, като директен маркетинг (непоискани рекламни съобщения);

10.7. да възразите срещу автоматизирана обработка, включително профилиране;

10.8. да не бъдете обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране;

10.9. да бъдете уведомени и да бъде поискано допълнителното Ви съгласие, ако данните Ви трябва да се обработват за цел различна от първоначалната;

10.10. да подадете жалба до надзорния орган - Комисия за защита на личните данни, адрес: гр. София 1592, бул. Проф. Цветан Лазаров № 2, електронна поща: kzld@cpdp.bg, интернет страница: (www.cdpd.bg);

10.11. да подадете жалба относно обработката на личните Ви данни чрез БСК, като използвате посочените данни за контакт.

11. БСК може да откаже заличаването на лични данни по следните причини:

11.1. при упражняване на правото на свобода на изразяването и правото на информация;

11.2. за спазване на законово задължение от страна на БСК или за изпълнението на задача от обществен интерес;

11.3. при упражняване на официални правомощия (ако е приложимо);

11.4. за установяването, упражняването или защитата на правни претенции.

12. Автоматизирано вземане на решения, включително профилиране – БСК не извършва автоматизирано вземане на решения, включително профилиране.

Долуподписаният/а

....., ЕГН.....

Заявявам, че съм запознат със съдържанието на настоящата информация.

Дата

Подпис

ДЕКЛАРАЦИЯ ЗА СЪГЛАСИЕ НА СУБЕКТА НА ДАННИТЕ

Долуподписан/ият/та.....,

(име на субекта на данните, друга информация за идентификация)

с настоящото декларирам, че

1. Давам съгласие на Българска стопанска камара-съюз на българския бизнес да обработва моите лични данни за целите на:

.....

2. Давам съгласие БСК да ми изпраща съобщения и покани за обучения , семинари и др.

3. Информиран съм, че мога да оттегля моето съгласие по всяко време.

4. Информиран съм, че оттеглянето на съгласието ми по-късно няма да засегне законосъобразността на обработването, основано на дадено сега съгласие.

Дата

Подпис

ОТТЕГЛЯНЕ НА СЪГЛАСИЕ ОТ СУБЕКТА НА ДАННИТЕ

Долуподписан/ият/та,.....

(три имена на субекта на данните, друга информация за идентификация и контакти),

в качеството си на „субект на лични данни“ и при условията на Общия регламент за защита на личните данни,

Като се има предвид, че:

съм предоставил съгласието си за обработване на следните лични данни

.....

(посочва се точно за какви лични данни е дадено съгласие)

по следния начин:.....

във връзка със следната цел:

от администратора на лични данни *Българска стопанска камара –сюз на българския бизнес*

и като заявявам, че съм надлежно информиран, че имам право да оттегля съгласието си за обработване на лични данни частично или изцяло по всяко време, без да съм задължен да посочвам причина за оттеглянето,

С НАСТОЯЩОТО ВИ УВЕДОМЯВАМ, ЧЕ:

Оттеглям съгласието си личните ми данни, посочени в това уведомление, да бъдат събирани и обработвани за посочената цел/цели.

Декларирам, че оттеглям своето съгласие за обработване на лични данни свободно, изрично и относно всички посочени лични данни, съгласно собствената си воля и убеждение.

Запознат съм, че имам право на възражения и жалби пред Комисия за защита на личните данни, която е надзорен орган в Република България, в случай, че администраторът на лични данни продължи обработването горепосочените данни след оттеглянето на съгласието с настоящото уведомление.

Дата

Подпис

СЪГЛАСИЕ ОТ РОДИТЕЛ / НАСТОЙНИК

Долуподписан/ият/та,

(три имена на родител/настойник, друга информация за идентификация)

в качеството си на родител/настойник, потвърждавам, че

.....

(три имена на детето, друга информация за идентификация)

е на възраст под 16 години и съм съгласен от негово име да се обработват личните му данни, за целите на:

от Българска стопанска камара – съюз на българския бизнес.

Информиран съм, че мога да оттегля настоящото съгласие по всяко време.

Известно ми е, че оттеглянето на съгласието ми по-късно няма да засегне законосъобразността на обработването, основано на даденото сега съгласие.

Дата

Подпис

ОТТЕГЛЯНЕ НА СЪГЛАСИЕ ОТ РОДИТЕЛ/НАСТОЙНИК

Долуподписан/ият/та,

(три имена на родител/настойник, друга информация за идентификация)

в качеството си на родител/настойник, оттеглям съгласието си да се обработват личните данни на,

(три имена на детето, друга информация за идентификация)

обработвани от *Българска стопанска камара – съюз на българския бизнес.*

Известно ми е, че оттеглянето на съгласието не засяга законосъобразността на обработката до този момент.

Разбирам, че обработката ще бъде спряна възможно най-бързо, ако не и веднага в онлайн автоматизирана среда. Въпреки това може да има разумно забавяне, докато заявката за изтегляне се обработва.

Запознат съм, че имам право на възражения и жалби пред Комисия за защита на личните данни, която е надзорен орган в Република България, в случай че администраторът на лични данни продължи обработването горепосочените данни след оттеглянето на съгласието с настоящото уведомление.

Дата

Подпис

ПРОЦЕДУРА ПО ПОЛУЧАВАНЕ НА СЪГЛАСИЕ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

I. Цел: определяне на реда за получаване на съгласие на субекта на данни за тяхното обработване, когато не се прилага друго правно основание.

II. Нормативна уредба: член 4, точка 11 от ОРЗД, член 7 и член 8 член 9, параграф 2, буква а от ОРЗД

III. Задължения: всички служители на БСК, които обработват лични данни; длъжностното лице по защита на данните/отговорникът по защита на данните следи за спазването на правилата за получаване на съгласието в съответствие с изискванията на настоящата процедура.

IV. Ход на процедурата

4.1. Получаване на съгласие от субекта на данните

4.1.1. Служителят на БСК, който осъществява дейност, за която е необходимо обработване на лични данни, предоставя на субектите на данни:

а/ информация относно обработване на лични данни на физически лица от БСК за да гарантира, че субектът на данни е информиран за правата си във връзка с обработката на личните му данни;

б/ образец на съгласие от субекта на данни.

4.1.2. Служителят на БСК изисква от субекта на данни:

а/ да се запознае с информацията относно обработване на лични данни на физически лица от БСК и да я подпише;

б/ да попълни формата на образец на съгласие, като посочи и за каква конкретна цел/и личните му данни могат да бъдат обработвани, както и че е информиран за правото си да оттегли съгласието, и, че оттеглянето на съгласието не засяга законосъобразността на обработването.

4. 2. Получаване на съгласие от дете

4.2.1. Получаване на съгласието от дете под 16- годишна възраст, се взема от родителя/настойника, по реда на т. 4.1.

4.3. За получаване на съгласията се използват образците публикувани на страницата на БСК.

ПРОЦЕДУРА ПО ОТТЕГЛЯНЕ НА СЪГЛАСИЕТО ОТ СУБЕКТА НА ДАННИ

- I. Цел: определяне на реда за оттегляне съгласието на субекта за обработка на личните му данни.
- II. Нормативна уредба Член 7 и член 8 от Общия регламент за защита на данните (ОРЗД)
- III. Задължения:
 - 3.1. БСК отговоря съгласно ОРЗД за администриране на оттеглянето на съгласието от субекта на данни.
 - 3.2. Всички служители на БСК, които обработват лични данни отговарят за спазване на процедурата по оттегляне на съгласие за обработване, ако съгласието е дадено пред тях.
 - 3.3. Длъжностното лице по защита на данните/Отговорникът по защита на данните следи за спазването на правилата за оттеглянето на съгласието в съответствие с изискванията на настоящата процедура.
- IV. Ход на процедурата
 - 4.1. Оттегляне на съгласие от субекта на данните
 - 4.1.1. При направено искане за оттегляне на съгласие, служителят обработващ лични данни получава подписаният по образец документ за оттегляне на съгласието за обработка на лични данни и го предава на Длъжностното лице/Отговорникът по защита на личните данни.
 - 4.1.2. БСК прекратява дейностите по обработка, които се основават на съгласието.
 - 4.1.3. Съответният служител на БСК е задължен да пази и съхранява документът с който е оттеглено съгласието за обработка на данни.
 - 4.2. Оттеглянето на съгласието може да бъде изцяло или само по отношение на една или повече конкретни цели на обработването.
 - 4.3. Процедурата е приложима и при оттегляне на съгласие за обработване на лични данни на лице под 16 – годишна възраст. Оттеглянето се извършва от родителя/настойника или лицето, чиито данни се обработват, след навършване на 18-годишна възраст.

ДЕКЛАРАЦИЯ ЗА ПОВЕРИТЕЛНОСТ

Долуподписан/ият/ата.....ЕГН.....

ДЕКЛАРИРАМ, ЧЕ

1. запознат/а съм с Политиката и Вътрешните правила на Българска стопанска камара-съюз на българския бизнес по защита на личните данни на физически лица¹ и се задължавам да я прилагам при изпълнение за служебните/договорните си ангажименти;
2. ще събирам и обработвам лични данни в обем, необходим за изпълнение на конкретни служебни/договорни ангажименти, единствено и само за целите на изпълняваната/възложена с договор дейност;
3. ще прилагам всички технически и организационни мерки, утвърдени от ръководството на БСК, описани в Политиката и Вътрешните правила, с оглед осигуряване на поверителност и конфиденциалност на личните данни на физическите лица;
4. задължавам се да не разкривам лични данни на трети страни, освен ако ръководството на БСК не е дало такива права на тази трета страна по договорна клауза за поверителност.
5. в случай на нарушение на сигурността на личните данни или на какъвто и да било друг инцидент, свързан със сигурността на данните се задължавам да уведомя служителя, отговарящ за защита на личните данни в БСК за предприемане на съответните действия;
6. известно ми е, че за нарушение на Политиката и Вътрешните правила нося отговорност за действително причинените вреди на субекта на данните и на БСК.

Дата

Подпис:

¹ Политиката и правилата са публично достъпна на интернет страницата на БСК www.bia-bg.com

ИСКАНЕ ОТ СУБЕКТ НА ДАННИТЕ

до администратора Българска стопанска камара – съюз на българския бизнес

Данни за физическото лице:

Трите имена: ЕГН:

Адрес:

телефонен номер: E-mail:

Пълномощно (нотариално заверено), ако искането се подава от пълномощник:

Данни за пълномощника:

Трите имена: ЕГН:

Адрес:

телефонен номер: E-mail:

Представител на субекта на данни:

Действате ли като представител от името на субекта на данни?	НЕ <input type="checkbox"/> ДА <input type="checkbox"/>	
Ако "Да", моля, посочете в качеството си на какъв (например родител, настойник, попечител, упълномощен представител)		
Данни на представителя:		
Три имена		
Дата на раждане		
Данни за контакт		
Държава		
Настоящ адрес		
Телефонен номер		
E-mail		
Допълнителни данни за идентификация на представителя:	<i>Моля, приложете доказателства [2], че сте законно упълномощени да получавате тази информация.</i>	
Вид на искането:		Описание на искането и данни, за които се отнася
Искане за достъп	ДА <input type="checkbox"/>	
Искане за коригиране	ДА <input type="checkbox"/>	
Искане за изтриване (право да бъдеш забравен)	ДА <input type="checkbox"/>	
Искане за ограничаване на обработването	ДА <input type="checkbox"/>	
Възражение срещу обработване	ДА <input type="checkbox"/>	
Искане за пренос на данни	ДА <input type="checkbox"/>	
Друго	ДА <input type="checkbox"/>	

2. ДЕКЛАРАЦИЯ

Аз, долуподписанияткато декларирам, че посочените по-горе данни са верни, с настоящото заявявам пред (име на администратора) искането ми, посочено по-горе, относно описаните данни.

Дата: Подпис:

Форма за искания , попълнен от (*име на служител*):

Аз, долуподписаният,, в качеството ми на представител, като декларирам, че посочените по-горе данни са верни, с настоящото заявявам пред (име на администратора) искането ми , посочено по-горе, относно описаните данни.

Дата: Подпис:

Получено от:.....на.....

ПРОЦЕДУРА ЗА УПРАВЛЕНИЕ НА ИСКАНИЯТА ОТ СУБЕКТИТЕ
отпавени до Българска стопанска камара-съюз на българския бизнес

- I.** Цел: осигуряване на своевременно обработване на исканията на субектите.
- II.** Обхват: процедурата се прилага по отношение на всички лични данни.
- III.** Искания: субектът на данни може в защита на своите права да отпави към БСК следните искания:
- Искане за достъп ;
 - Искане за коригиране;
 - Искане за изтриване („право да бъдеш забравен“);
 - Искане за ограничаване на обработването;
 - Искане за пренасяне на данните;
 - Възражение срещу обработване.

II. Нормативна уредба : членове 12, 15, 16, 17, 18, 20 и 21 от Общия регламент за защита на данните (ОРЗД).

III. Задължения: лъжностното лице по защита на данните/отговорникът по защита на данните отговаря за прилагането и ефективното изпълнение и обработката на всички искания обхванати от на тази процедура.

IV. Ход на процедурата

4.1. Отпавяне на искане от субекта на данните

4.1.1. Исканията се правят, като за улеснение се използва Образец на форма за искане от субект на данните.

4.1.2. При отпавянето на искане се спазват следните правила:

а/ субектът на данни указва конкретния вид искане, съдържащ се в образеца на формата, предоставена от БСК;

б/ субектът на данните може да поиска всички негови лични данни, съхранявани от БСК без да указва конкретен вид;

в/ субектът на данните предоставя на БСК данни за самоличността си, които да го идентифицират сигурно и еднозначно (данни от лични документи, клиентски номер, електронна идентификационна карта и т.н).

г/ БСК задължително проверява идентификационните данни, за да се увери, че искането е подадено от субекта, който данните идентифицират;

д/ БСК документира датата на получаване на искането;

е/ След като искането бъде получено, то незабавно се препраща до Длъжностното лице по защита на данните / Отговорника по защита на данните, който задвижва процеса по обработка на искането и изпращането на отговор на субекта на данните.

4.2. Обработка на искането

4.2.1. Обработката на искането се извършва по следния начин:

а/ длъжностното лице по защита на данните/отговорникът по защита на данните поддържа Регистър на исканията от субекти на данните;

б/ длъжностното лице по защита на данните/отговорникът по защита на данните вписва в Регистъра на исканията от субекти на данните датата, идентифициращата информация и всички други важни за разглеждане на искането данни;

в/ идентифицирането (търсенето) на личните данни се извършва във всички информационни масиви с данни и всички съответни системи за архивиране, включително всички архивирани файлове;

г/ длъжностното лице по защита на данните / Отговорникът по защита на данните извършва обработване на данните с цел отстраняване на евентуална идентификационна информация за трети лица.

е/БСК предоставя исканата информация и отговаря на исканията на субекта на данните в рамките най-късно на един месец от датата на получаване на искането за достъп.

ж/длъжностното лице за защита на данните/отговорникът за защита на данните вписва в Регистъра на исканията данни за подадения към субекта отговор на искането за достъп.

4.3. Допълнителна информация, изпращана при искане за достъп

4.3.1. В случай на искане от субекта на данни за получаване на достъп до данните, освен че осигурява достъп до данните (например, чрез предоставяне на тяхно копие), БСК изпраща на субекта и следната информация:

а/ целите на обработването;

б/съответните категории лични данни, които се обработват;

в/получателите или категориите получатели на личните данни (ако има такива);

г/информация относно намерението на БСК да предаде данните на трета държава или на международна организация, както и наличието на гаранции за защита на данните;

д/ срока, за който БСК ще съхранява личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок;

е/правата му да се изиска от БСК коригиране или изтриване на неговите лични данни, както и правата му на ограничаване на обработването, на възражение срещу обработването, както и на преносимост на данните;

ж/ правото на жалба до надзорен орган;

з/ когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник;

4.3.2. Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повтаряемост, Длъжностното лице по защита на данните / Отговорника по защита на данните може:

а/да предложи на ръководството на БСК да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или комуникацията или предприемането на исканите действия;

б/да откаже да предприеме действия по искането.

4.4. Действия при искания за коригиране, изтриване или ограничаване и при възражения срещу обработването

4.4.1. При искане на субекта на данни за коригиране, изтриване, ограничаване или при възражение по отношение на обработваните лични данни Длъжностното лице по защита на данните / Отговорникът за защита на данните отговаря да бъде преценено всяко от тези искания (извън искането за достъп до данни) с оглед основателността на правото на субекта и наличието на други законови изисквания за неговото удовлетворяване.

4.4.1. След постъпването на съответното искане:

а/ БСК премахва личните данни от системите и прекратява операциите по обработката им, без ненужно забавяне, ако искането за изтриване е подадено от субекта на данните;

б/ БСК съобщава за всяко извършено коригиране, изтриване или ограничаване на обработването на всеки получател, на когото личните данни са били разкрити с писмено уведомление на хартиен носител или по електронна поща;

в/ БСК информира субекта на данните относно тези получатели, ако субектът на данните поиска това, и документира това съобщение;

г/ БСК взема подходящи мерки, без ненужно забавяне, в случай че:

о субектът на данни е подал искане, с което възразява срещу обработването на личните данни изцяло или частично;

о отпаднало е основанието за обработка по законово задължение;

о данните са били незаконно обработвани.

ПРОЦЕДУРА ЗА НАЧИНИТЕ НА КОМУНИКАЦИЯ ПРИ ЖАЛБИ И ИСКАНИЯ ОТ СУБЕКТА НА ДАННИ

I. Цел: определя реда за разглеждане на:

1. жалби и искания от субекти на данни, свързани с обработката на техните лични данни от БСК;
2. обработка на искания от субектите на данни относно упражняването на техните права по ОРЗД;
3. жалби на субектите на данни относно начина на обработване на техните искания или жалби.

II. Нормативна уредба: член 12 от Общия регламент за защита на данните (ОРЗД).

III. Задължения:

3.1. Всички служители / членове на персонала в БСК са отговорни за начина, по който жалбите и исканията, направени от субекти на лични данни, се изпращат по съответния ред до Длъжностното лице по защита на данните / Отговорника по защита на данните.

3.2. Длъжностното лице по защита на данните / Отговорникът по защита на данните отговаря за разглеждането на всички искания и жалби в съответствие с предписанията на тази процедура.

IV. Ход на процедурата

4.1. Обща информация и съобщения

4.1.1. БСК обявява координатите за контакт със своето Длъжностно лице по защита на данните / Отговорник по защита на данните, като ги публикува на своята интернет страница.

4.1.2. БСК поставя ясни и разбираеми указания на интернет страницата си относно подаването на искания и жалби, като публикува Образец на форма за искане от субект на данните.

4.1.3. БСК предоставя публичен достъп на субектите на данните до своята Декларация за поверителност (уведомление за поверително третиране на личните данни) .

4.1.4. БСК документира всички действия във връзка с комуникацията със субектите на данни в Регистъра на исканията.

4.2. Възможности на субекта на данни

4.2.1. Субектите на данни могат да подадат до БСК:

а/ искания за осъществяване на правата им по защита на личните данни – искане за достъп, за изтриване, за ограничаване на обработването, възражение за обработване, за пренос на данните;

б/ оплаквания относно начина на разглеждане на искането им за достъп до данните;

в/ оплаквания относно начина на разглеждане на искането/жалбата им;

г/ жалба срещу всяко решение, взето след подадено искане/жалба.

4.3. Начин на подаване на искания и жалби

4.3.1. Субектите на данни отправят искания и жалби чрез Образец за искане от субект на данните публикувана на интернет страницата на БСК.

4.4. Отговор и срокове

4.4.1. БСК разглежда и взема решение по постъпилото искане или жалба при спазване на следните правила и срокове:

а/ исканията/жалбите се насочват към Длъжностното лице по защита на данните / Отговорника по защита на данните, който трябва да вземе решение и да даде отговор на субекта на данните най-късно в срок от един месец от тяхното получаване;

б/ жалбата срещу взетото решение трябва да бъде разгледана и решена в срок от 14 дни, като по изключение срокът може да бъде удължен до 30 дни;

в/ БСК ако не удовлетвори искането на субекта на данни в рамките на изискуемите срокове или откаже да уважи жалбата, то в отговора си излага на ясен и разбираем език причините, поради които не е предприел действие или е отказал.

4.4.2. БСК също така информира в отговора си субекта на данните относно тяхното право да подават жалби директно до надзорния орган – Комисията за защита на личните данни.

4.4.3. Всички действия на БСК предприети в изпълнение на настоящата процедура, се извършват без да се дължи заплащане от субекта на данните.

ПРОЦЕДУРА ЗА ПРЕНОСИМОСТ НА ДАННИ

I. Цел: определяне на реда по който субектът на данни упражнява своето право на преносимост на личните си данни по отношение на БСК, като поиска БСК да предостави тези данни на друг администратор, посочен от субекта.

II. Обхват: процедурата се прилага само за тези лични данни, за които субектът на данните е дал съгласие за обработване или обработването им е било необходимо за сключването и изпълнението на договор или обработването им е било извършено по автоматизиран начин.

Процедурата се прилага и за получаване на данни от БСК от друг администратор.

III. Нормативна уредба: член 12 от Общия регламент за защита на данните (ОРЗД)

IV. Задължения: БСК, Длъжностното лице по защита на данните / Отговорникът по защита на данните и ръководителя на ИТ отдела /когато е приложимо/ отговарят за спазване на процедурата и прехвърляне на данните при спазване на комуникационна ситуираност.

V. Ход на процедурата

5.1. Предаване на лични данни или прехвърляне към друг администратор

5.1.1. БСК информира субектите на данни за съществуването на право на преносимост към момента на получаване на лични данни.

5.1.2. При постъпване на искане за предаване или за прехвърляне на лични данни към друг администратор, БСК обработва искането при спазване на следните правила:

а/всяко постъпило искане незабавно се изпраща на Длъжностното лице по защита на данните / Отговорника по защита на данните, който проверява за ясни и неоспорими доказателства за самоличността на субекта на данни под формата на лични документи, клиентски номер, електронна карта или друг еднозначен идентификатор;

б/длъжностното лице по защита на данните / Отговорникът по защита на данните проверява дали посочените от субекта данни са получени на основание съгласие или договор и дали са обработени по автоматизиран начин. Ако не са изпълнени тези изисквания, БСК има право да откаже да удовлетвори искането;

в/когато исканите данни засягат трето лица/а, Длъжностното лице по защита на данните / Отговорникът по защита на данните преценява дали предаването на данни на друг администратор на лични данни би навредило на правата и свободите на други субекти на данни;

г/длъжностното лице по защита на данните / Отговорникът по защита на данните извършва проверка дали подготвените за предаване/прехвърляне лични данни са само и точно тези, които субектът на данни е поискал да бъдат предадени, респ. прехвърлени;

д/поисканата информация се предоставя на субекта на данни в структуриран, широко използван и машинно четим формат който позволява ефективно повторно използване на данните;

е/при предаване на данните на друг администратор на данни, БСК ги препраща в оперативно съвместим формат. В случай, че са налице технически пречки, които възпрепятстват директното им прехвърляне, БСК обяснява тези пречки на субекта на данните;

5.1.3. БСК предоставя исканата информация в рамките на един месец от датата на заявката. Ако заявката е сложна, БСК може да удължи тази времева рамка максимум до три месеца от датата на предявяването ѝ. БСК информира субекта на данни за причините за забавянето чрез писмено уведомление на хартиен носител или по електронна поща.

5.1.4. Длъжностното лице по защита на данните/Отговорникът по защита на данните поддържа записи за исканията за прехвърляне на данни в Регистъра на исканията, включително по дати.

5.2. Получаване на лични данни

5.2.1. БСК приема и съхранява само данните, които са необходими и относими към предоставяната услуга.

5.2.2. БСК не приема и не обработва лични данни „по подразбиране“, дори когато са получени от друг администратор след искане за прехвърлянето им, както и не съхранява всички получени данни.

5.2.3. Ако получените данни съдържат данни от трети лица, БСК съхранява данните под контрола на субекта заявител. Тези данни се управляват само за неговите нужди, но не и за други цели на БСК.

**ПРОЦЕДУРА ПО ПРЕДАВАНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ДЪРЖАВИ ИЛИ
МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ**

I. Цел: процедурата определя реда за предаване на лични данни от БСК на държави, които не са членки на ЕС и на международни организации.

II. Нормативна уредба: член 49 от Общия регламент за защита на данните (ОРЗД)

III. Задължения: отговорността за спазването на настоящата процедура е на БСК и длъжностното лице/отговорника по запазване на личните данни.

IV. Ход на процедурата

4.1. При предаване на лични данни на трети държави или международни организации, БСК извършва проверка дали е осигурено адекватно ниво на защита. Такова е налице, ако е изпълнено едно от следните изисквания на ОРЗД:

а/държавата / международната организация – получател на данните, респ. съответният икономически сектор в тази държава, е включена в одобрения списък на Европейския съюз с държави, сектори и международни организации, който се публикува в Официален вестник на ЕС;

б/държавата на получателя осигурява адекватни средства за защита на личните данни, установени с нормативна уредба или режим на саморегулация;

в/БСК има сключен договор, който съдържа стандартни клаузи за защита на данните, приети от Комисията, гарантиращи адекватно ниво на защита;

4.2. Освен в гореизброените случаи, БСК може да осъществи предаването въз основа на разрешение, дадено от надзорния орган, когато са предвидени подходящи гаранции за правата на физическите лица посредством:

а/договорни клаузи между БСК и администратора, обработващия лични данни или получателя на личните данни в третата държава или международната организация; или

б/разпоредби, които са включени в административните договорености между публичните органи или структури, съдържащи действителни и приложими права на субектите на данни.

4.3. По изключение, когато не са налице условията по т. 1 и 2 по-горе, БСК може да осъществи предаване на лични данни на трети държави или международни организации само и единствено при стриктно спазване на условията, предвидени в член 49 от ОРЗД и Политиката за защита на данните.

ПРОЦЕДУРА ЗА УВЕДОМЯВАНЕ В СЛУЧАЙ НА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

I. Цел: Настоящата процедура има за цел да противодейства срещу неправомерно обработване на личните данни на физическите лица и установява реда за реагиране и уведомяване в случай на нарушение сигурността на личните данни.

II. УВЕДОМЯВАНЕ НА НАДЗОРНИЯ ОРГАН

2.1. В случай на нарушение на сигурността на личните данни администраторът, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа, след като е разбрал за нарушението, уведомява Комисията за защита на личните данни. Уведомлението до комисията съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

2.2. Обработващият лични данни уведомява администратора без ненужно забавяне, след като узнае за нарушаване на сигурността на лични данни.

2.3. В уведомлението се съдържа информацията относно:

- Описание на естеството на нарушението и в какво се състои то;
- Категориите и приблизителния брой засегнати субекти на данни;
- Категориите и приблизителния брой засегнати записи на лични данни;
- Лице за контакт, от което може да бъде получена повече информация по случая;
- Описание на евентуалните последици от нарушението на сигурността на данните;
- Описание на предприетите мерки за справяне с нарушението и отстраняване на неблагоприятните последици.

III. УВЕДОМЯВАНЕ НА СУБЕКТА НА ДАННИТЕ

3.1. Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът, без ненужно забавяне, изпраща на субекта на данните съобщение за нарушението. Съобщението се изпраща по електронна поща, когато е налична информация за такава или с пощенска/куриерска услуга. В съобщението на ясен и разбираем език се описва естеството на нарушението на сигурността на личните данни и се предоставя информацията, посочена в чл. 4 от настоящата процедура.

3.2. Изпращане на съобщение до субекта на данните не се изисква, ако някое от следните условия е изпълнено:

- предприети са подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността като напр. мерки, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;
- впоследствие са взети мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;
- изпращането на съобщение е свързано с непреодолими пречки и би довело до непропорционални усилия – в този случай се прави публично съобщение до всички засегнати субекти.

**УВЕДОМЛЕНИЕ ОТ АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ ДО НАДЗОРНИЯ ОРГАН ЗА
НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ**

ДО:

Надзорен орган:

На вниманието на

Информация за Администратора

Наименование

ЕИК/БУЛСТАТ/ЕГН

Адрес:

Данни за контакт с Длъжностно лице по защита на данните/Отговорник по защита на данните:

Три имена

Телефон

E-mail

Адрес

Друга информация за контакт:

Описание на естеството на нарушението на сигурността на личните данни:

Дата и час на узнаване на нарушението:

Причина за забавяне на уведомяването (*ако има такова*)

.....

Описание

.....

Категории засегнати лични данни

.....

Засегнати субекти (*категории и приблизителен брой*)

.....

Засегнати записи на лични данни (*приблизителен брой*)

.....

Последици от нарушение на сигурността на личните данни

.....

Поетапно подаване на информация – ДА / НЕ

.....

Предприети или предложени от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност, мерки за намаляване на евентуалните неблагоприятни последици

.....

Доказателства (описание)

.....

Оценка на риска/ технически организационни мерки

.....

Дата:

Подпис:

ПРОЦЕДУРА ЗА СЪХРАНЯВАНЕ И УНИЩОЖАВАНЕ НА ДАННИТЕ

I. Цел: осигуряване на съхраняване и унищожаване на лични данни обработвани от БСК.

II. Нормативна уредба:

2.1. Член 5, параграф 1, буква д) и член 30, параграф 1, буква е) от Общия регламент за защита данните (ОРЗД);

2.2. Глава трета от Закона за националния архивен фонд;

2.3. Наредба за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общинските институции.

III. Задължения:

3.1. Главният финансов директор отговаря за съхраняването на финансовите (счетоводни, осигурителни, данъчни) и свързаните с тях записи и документи.

3.2. Лицето осъществяващо дейност свързана с човешки ресурси отговаря за съхраняването на данните по набиране на персонал, освобождаване, оформяне на документи за трудов стаж и др.

3.3. Ръководителят на Правния отдел е отговорен за запазването на всички документи от правен характер, които не се съхраняват в руги отдели.

3.4. Всеки ръководител на отдел/програма е отговорен за съхраняване на данните събирани във връзка с осъществяваната от отдела/програмата дейност.

3.5. Длъжностното лице по защита на данните / Отговорникът по защита на данните носи отговорност за съхраняването на данни в съответствие с тази процедура.

IV. Ход на процедурата

4.1. Изискваните срокове на съхраняване по вид на записа се записват в График за съхраняване и унищожаване на категориите лични данни, както следва:

а/ вид на носител на данни;

б/ срок на съхранение;

в/ основание за срока;

г/ метод на унищожаване;

4.2. Длъжностното лице по защита на данните / Отговорникът по защита на данните записва предвидените срокове за изтриване на различните категории данни в Регистъра на дейностите по обработване, съгласно член 30, параграф 1, буква е) от ОРЗД, винаги, когато това е възможно.

4.3. Длъжностното лице по защита на данните / Отговорникът по защита на данните са отговорни за унищожаването на данните, след като е изтекъл срокът на съхранение, както е посочено в графика за съхранение и унищожаване.

4.4. Унищожаването се извършва по следния начин:

а/ изтриване на информацията върху записващи носители;

б/ бракуване на записващи носители, за което се съставя протокол.