БЪЛГАРСКА АСОЦИАЦИЯ НА УПРАВЛЕНСКИТЕ КОНСУЛТАНТСКИ ОРГАНИЗАЦИИ
пл. „Славейков“ 6, етаж 2, 1000 София, България
bamco@bamco.bg, bamco.bg

Политика за защита на личните данни

Съдържание

1. Общи положения, цели и обхват 2
2. Свързани нормативни и вътрешни актове 3
3. Понятия 4
4. Управленска ангажираност и роли по Регламент (ЕС) 2016/679 6
5. Принципи за защита на данните 7
5.1. Законосъобразност, добросъвестност и прозрачност 7
5.2. Ограничаване до целите 8
5.3. Свеждане на данните до минимум 8
5.4. Точност 8
5.5. Ограничение на съхранението 9
5.6. Цялостност и поверителност 9
Поверителност (Чл. 32, ал. 1 т.б от GDPR) 10
Цялостност (Чл. 32, ал.1, т.б от GDPR) 10
Общи мерки 11
5.7. Отчетност 12
6. Права на субектите на данни 13
7. Съгласие 14
8. Сигурност на данните 15
9. Разкриване на данни 16
10. Съхраняване и унищожаване на данните 17
11. Трансфер на данни 18
11.1. Решение за адекватност 18
11.2. Щит за личните данни в отношенията между ЕС и САЩ (EU-U.S. Privacy Shield) 18
11.3. Задължителни фирмени правила 18
11.4. Стандартни договорни клаузи 19
11.5. Изключения 19
12. Регистър на дейностите по обработване на лични данни 20
13. Влизане в сила и актуализация 20

1. Общи положения, цели и обхват

Тази политика има за цел да въведе основните принципи за обработване на личните данни и да гарантира правата на субектите на данни в тази връзка.

Ръководството на БАУКО, се ангажира да осигури съответствие със законодателството на ЕС и държавите-членки по отношение на обработването на личните данни и защитата на "правата и свободите" на лицата, чиито лични данни БАУКО събира и обработва съгласно Общия регламент за защита на данните (Регламент (ЕС) 2016/679).

В съответствие с Общия регламент към тази политика са описани и други релевантни документи, както и свързани процеси и процедури.

Политиката има задължителен характер за сдружението като организация, за неговите членове, управителни органи, служители, контрагенти и трети лица по отношение на личните данни, които се обработват във връзка с дейността на БАУКО. Отговорност на всички гореизброени е да се запознаят с тази политика и да гарантират адекватното й спазване.

Регламент (ЕС) 2016/679 и тази политика се отнасят до всички дейности по обработването на лични данни , включително тези, които се извършват относно лични данни на клиенти, служители, доставчици и партньори и всякакви други лични данни, които организацията обработва от различни източници. Тази политика обхваща всички бизнес процеси в организацията на БАУКО.

Спазването на законодателството за защита на данните е отговорност на всички гореизброени лица, които обработват лични данни.

Всяко нарушение на настоящата политика ще бъде разглеждано като нарушение на трудовата дисциплина.

Партньори и трети лица, които работят с БАУКО, както и които имат или могат да имат достъп до личните данни, са длъжни да се запознаят и да се съобразят с тази политика. Никоя трета страна не може да има достъп до лични данни, съхранявани от БАУКО, без предварително да е сключила споразумение за поверителност на данните. Като администратор на лични данни, БАУКО има право да извършва проверки на спазването на наложените със споразумението задължения.

2. Свързани нормативни и вътрешни актове

- EU GDPR 2016/679 (Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. за защита на физическите лица при обработването на лични данни и за свободното движение на такива данни и за отмяна на Директива 95/46 / ЕО)
- Закон за защита на личните данни
- Насоки/Методически указания на Комисията за защита на личните данни
- Политика за съхранение на личните данни

3. 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 комбиниране, ограничаване, изтриване или унищожаване;
- „Администратор" - всяко физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на ЕС или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка;
- „Обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;
- „Субект на данните“ – всяко живо 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“ – Общият Регламент определя дете като всеки на възраст под 16 години въпреки че това може да бъде намалена на 13 от правото на държавата-членка. Обработката на лични данни на едно дете е законно само, ако родител или попечител е дал съгласие. Администраторът полага разумни усилия, за да провери в

такива случаи, че притежателят на родителската отговорност за детето е дал или упълномощен да даде съгласието си.

- „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;
- „Основно място на установяване “ – седалището на администратора в ЕС ще бъде мястото, в което той взема основните решения за целта и средствата на своите дейности по обработване на данни. По отношение на обработващия лични данни основното му място на установяване в ЕС ще бъде неговият административен център.
- Ако администраторът е със седалище извън ЕС, той трябва да назначи свой представител в юрисдикцията, в която администраторът работи, за да действа от името на администратора и да се занимава с надзорните органи. (Член 4 т.16) от ОРЗД)
- „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;
- Виж чл. 4 от ОРЗД, където са дадени определенията за всяко от горните.

4. Управленска ангажираност и роли по Регламент (ЕС) 2016/679

4. 1. БАУКО е администратор на данни и/или , обработващ данни в зависимост от начина на обработване на лични данни, определен в Регламент (ЕС) 2016/679.

4.2. Висшето ръководство и всички членове на управителните органи БАУКО са отговорни за разработване и насърчаване на добри практики в областта на обработване на лични данни в БАУКО;

5. Принципи за защита на данните

Обработването на лични данни трябва да се извършва в съответствие с принципите за защита на данните, посочени в член 5 от Регламент (ЕС) 2016/679. Политиките и процедурите на БАУКО имат за цел да гарантират спазването на тези принципи.

5.1. Законосъобразност, добросъвестност и прозрачност

Личните данни трябва да бъдат обработвани законосъобразно, добросъвестно и прозрачно.

Законосъобразно – наличие на валидно правно основание за обработването на лични данни. Това основание може да бъде спазването на законово задължение на БАУКО, изпълнението на договор, идентифициран легитимен интерес на БАУКО, съгласие на субекта на данните, за изпълнението на задача от обществен интерес.

Добросъвестно - за да може обработването да бъде добросъвестно, администраторът на данни трябва да предостави определена информация на субектите на данни, доколкото това е практически възможно. Това важи независимо дали личните данни са получени директно от субектите на данни или от други източници.

Регламент (ЕС) 2016/679 увеличава изискванията за това каква информация трябва да бъде на разположение на субектите на данни, която е обхваната от изискването за "прозрачност".

Прозрачно – Общият регламент включва правила относно предоставяне на информация на субектите на данни в членове 12, 13 и 14 от ОРЗД. Информацията трябва да бъде съобщена на субекта на данните в разбираема форма, като се използва ясен и разбираем език.

Информацията се предоставя по подходящ начин чрез уведомление за поверително третиране на личните данни.

Специфичната информация, която трябва да бъде предоставена на субекта на данните, трябва да включва като минимум:

- данни, които идентифицират администратора и данните за контакт на администратора и, ако има такъв, на представителя на администратора;
- целите на обработването, за което личните данни са предназначени както и правното основание за обработването;
- периода, за който ще се съхраняват личните данни;
- съществуването на следните права - да поиска достъп до данните, коригиране, изтриване (право „да бъдеш забравен“), ограничаване на обработването, както

право на възражение срещу условията (или липсата на такива) във връзка с упражняването на тези права;

- категориите лични данни;
- получателите или категориите получатели на лични данни, където това е приложимо;
- където е приложимо, дали администраторът възнамерява да прехвърли личните данни към получател в трета страна и нивото на защита на данните;
- всякаква допълнителна информация, необходима да се гарантира добросъвестно обработване.

5.2. Ограничаване до целите

Лични данни могат да се събират само за конкретни, изрично указани и законни цели.

Данните, получени за конкретни цели, не трябва да се използват за цел, която се различава от тези, описани в Регистъра на дейностите по обработване на данни (чл. 30 ОРЗД) на БАУКО.

5.3. Свеждане на данните до минимум

Личните данни трябва да бъдат достатъчни, относими и ограничени до това, което е необходимо за обработването им за съответната цел.

5.4. Точност

Личните данни трябва да бъдат точни и актуализирани своевременно, и да са положени необходими усилия, за да е възможно незабавно (в рамките на възможните технически решения) изтриване или коригиране.

Данните, които се съхраняват от администратора на данни, трябва да бъдат преглеждани и актуализирани при необходимост. Не трябва да се съхраняват данни, в случаите, когато има вероятност да не са точни.

От служителите / работниците (клиентите / други) бъде изисквано да уведомяват БАУКО за всякакви промени в обстоятелствата, за да могат да се актуализират записите на лични данни. Отговорността на БАУКО е да гарантира, че всяко уведомление относно промяната на обстоятелствата е записано и се предприемат действия.

На годишна база, определен от Председателя на УС координатор на БАУКО, ще прегледа сроковете на съхранение на всички лични данни, обработвани от БАУКО, като се позовава на инвентаризацията на данните и ще идентифицира всички данни, които вече не

се изискват в контекста на съответната цел. Тези данни ще бъдат надеждно унищожени в съответствие с процедурите и правилата на администратора.

Определен от Председателя на УС координатор на БАУКО е отговорен за съответствие с искания за корекция на данни в рамките на един месец. Ако БАУКО реши да не се съобрази с искането, определеният координатор на БАУКО трябва да отговори на субекта на данните, за да обясни мотивите за взетото решение и да го информира за правото му да подаде жалба пред надзорния орган, и да потърси правна защита.

Определен от Председателя на УС координатор на БАУКО, е отговорен за вземане на подходящи мерки, в случаите когато организациите на трети страни имат неточни или остарели лични данни, да ги информира, че информацията е неточна или остаряла и е да не се използва за вземане на решения относно лицата, да информира съответните страни; и да препраща всяка корекция на лични данни към третите страни, където това е необходимо.

5.5. Ограничение на съхранението

Личните данни трябва да се съхраняват в такава форма, че субектът на данните може да бъде идентифициран само толкова дълго, колкото е необходимо за целите на обработването.

Когато личните данни се запазват след датата на обработването, те ще бъдат съхранявани по подходящ начин (минимизирани, криптирани, псевдонимизирани), за да се защити самоличността на субекта на данните в случай на нарушение на данните.

Лични данни ще бъдат пазени в съответствие с Процедура за съхранение на личните данни и след като е преминал срокът им на съхранение, те трябва да бъдат надеждно унищожени по указания в тази процедура ред.

5.6. Цялостност и поверителност

Личните данни трябва да бъдат обработени по начин, който гарантира подходяща сигурност.

При определянето на това доколко уместно е обработването трябва също така да се разгледа степента на евентуална вреда или загуба, която може да бъде причинена на физически лица (напр. персонал или клиенти), ако възникне нарушение на сигурността, както и всяка вероятна вреда за репутацията на администратора, включително евентуална загуба на доверие на клиентите.

За гарантиране на цялостността и сигурността на личните данни, БАУКО въвежда следните технически и организационни мерки:

Поверителност (Чл. 32, ал. 1 т.б от GDPR)

- Контрол на физическия достъп:

Не трябва да се допуска неоторизиран достъп до съоръженията за обработване на данни, напр.: магнитни или чип карти, ключове, електронни ключалки, услуги по сигурността и/или охрана на входовете, алармени системи, системи за видео наблюдение

- Контрол на електронния достъп:

Не трябва да се допуска неоторизирана употреба на системите за обработване и съхранение на данни, напр.: пароли, автоматични механизми за блокиране/заключване, двойно удостоверяване, криптиране на носителите на данни.

- Контрол на вътрешния достъп (разрешения за права на потребителите за достъп и корекция на данни):

Не трябва да се допуска неоторизирано четене, копиране, изменения или заличаване на данни в системата, т.е. оторизация на правата, права на достъп само до необходимата степен, записване на достъпа до системата

- Контрол чрез изолиране:

Изолираното обработване на данни, която се събира за различни цели, напр. поддръжка на множество клиенти, използване на тестова среда;

Цялостност (Чл. 32, ал.1, т.б от GDPR)

- Контрол на прехвърлянето на данните:

Не трябва да се допуска неоторизирано четене, копиране, изменения или заличаване на данни с електронно прехвърляне или транспорт, напр. криптиране, виртуални частни мрежи (VPN), електронен подпис;

Наличност и устойчивост (Чл. 32, ал.1 т.б от GDPR)

- Контрол на наличността:

Предотвратяване на случайно или умишлено унищожаване или загуба, напр. Стратегия за архивиране на резервни копия (онлайн/офлайн; на място/извън обекта), Непрекъснато подаване на електричество (UPS), защита от вируси, firewall, процедури за докладване и планиране за извънредни ситуации.

Общи мерки

- Защита с парола;
- Автоматично заключване на бездействащи работни станции в мрежата;
- Антивирусен софтуер и защитни стени;
- Правата за достъп основани на роли, включително тези, на назначен временно персонал
- Защитата на устройства, които напускат помещенията на организацията като лаптопи или други;
- Когато е подходящо - технологии за подобряване на поверителността, като например псевдонимизиране и анонимизиране;
- Идентифициране на подходящи международни стандарти за сигурност подходящи за БАУКО.

При оценяването на подходящите организационни мерки определен от Председателя на УС координатор на БАУКО ще вземе предвид следното:

- Нивата на подходящо обучение в БАУКО;
- Мерките, които отчитат надеждността на служителите (например атестационни оценки, препоръки и т.н.);
- Включването на защитата на данните в трудовите договори;
- Идентификация на дисциплинарни мерки за нарушения по отношение на обработването на данни;
- Редовна проверка на персонала за спазване на съответните стандарти за сигурност;
- Контрол на физическия достъп до електронни и хартиено базирани записи;
- Приемането на политика на „чисто работно място“ ;
- Съхраняване на хартия на базата данни в заключващи се стенни шкафове;
- Ограничаване на използването на портативни електронни устройства извън работното място;
- Ограничаване на използването от служителите на лични устройства на работното място;
- Приемане на ясни правила за създаване и ползване на пароли;
- Редовно създаване на резервни копия на личните данни и физическо съхраняване на носителите с копия извън офиса;
- Налагане на договорни задължения на организации контрагенти да предприемат подходящи мерки за сигурност при прехвърляне на данни извън ЕС.
- Тези контроли са избрани въз основа на идентифицираните рискове за лични данни, както и потенциала за нанасяне на вреди, на лицата, чиито данни се обработват.

5.7. Отчетност

Регламент (ЕС) 2016/679 включва разпоредби, които насърчават отчетността и управляемостта и допълват изискванията за прозрачност. Принципът на отчетност в чл. 5, пар. 2 изисква от администратора да докаже, че спазва останалите принципите в ОРЗД и изрично заявява, че това е негова отговорност.

БАУКО ще доказва спазването на принципите за защита на данните чрез прилагане на политики по защита на данните, като се присъединява към кодекси за поведение, внедрява подходящи технически и организационни мерки, както и чрез приемане на техники по защита на данните на етапа на проектирането и защита на данните по подразбиране, оценка на въздействието върху защитата на личните данни, процедура за уведомяване за нарушаване на лични данни и т.н.

6. Права на субектите на данни

6. 1. Субектите на данни имат следните права по отношение на обработването на данни, както и на данните, които се записват за тях:

- Да отправя искания за потвърждаване дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните, както и информация кои са получателите на тези данни.
- Да поиска копие от своите лични данни от администратора;
- Да иска от администратора коригиране на лични данни когато те са неточни, както и когато не са вече актуални;
- Да изиска от администратора изтриване на лични данни (право „да бъдеш забравен");
- Да иска от администратора ограничаване на обработването на лични данни като в този случай данните ще бъдат само съхранявани, но не и обработвани.;
- Да направи възражение срещу обработване на негови лични данни;
- Да направи възражение срещу обработване на лични данни, отнасящо се до него за целите на директния маркетинг.
- Да подаде жалба до надзорен орган ако смята, че някоя от разпоредбите на регламента е нарушена;
- Да поиска и да му бъдат предоставени личните данни в структуриран, широко използван и пригоден за машинно четене формат;
- Да оттегли съгласието си за обработката на личните данни по всяко време с отделно искане, отправено до администратора;
- Да не е обект на автоматизирано взети решения, които да го засягат в значителна степен, без възможност за човешка намеса;
- Да се противопостави на автоматизирано профилиране, което се случва без негово съгласие;

6.2. БАУКО осигурява условия, които да гарантират упражняването на тези права от субекта на данни:

- Субектите на данни могат да направят искания за достъп до данни, както е описано в „Процедура за обработване на исканията от субектите на данни и даване на съгласие“.
- Субектите на данни имат право да подават жалби до БАУКО, свързани с обработването на личните им данни и обработването на искане от субекта на данни

7. Съгласие

7.1. „Съгласие“ означава всяко свободно изразено, конкретно, информирано и недвусмислено изразяване на волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени. Субектът на данните може да оттегли своето съгласие по всяко време.

7.2. БАУКО счита за валидно "съгласие" само случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие и без върху него да бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация, няма да бъде валидно основание за обработване на лични данни.

7.3. Съгласието не може да бъде изведено от липсата на отговор на съобщение до субекта на данни. Трябва да има активна комуникация между администратора и субекта, за да е налице съгласие. Администраторът трябва да може да докаже, че е получено съгласие за дейностите по обработване.

7.4. За специални категории данни трябва да се получи изрично писмено съгласие на субектите на данни, освен ако не съществува алтернативно законно основание за обработване.

7.5. В повечето случаи съгласието за обработване на лични и специални категории данни се получава рутинно от БАУКО, като се използват стандартни документи за съгласие напр. когато е подадено заявление за приемане на нов член и др.

7.6. „Процедура за обработване на исканията от субектите на данни и даване на съгласие“ урежда реда за получаване и оттегляне на съгласие.

8. Сигурност на данните

8.1. Всички служители, членове на комисии, членове на сдружението и на управителните органи на БАУКО са отговорни за гарантирането на сигурността при съхраняването на данните, за които те отговарят и които БАУКО държи, както и, че данните се съхраняват сигурно и не се разкриват при каквито и да било обстоятелства на трети страни, освен ако БАУКО не е дал такива права на тази трета страна, като са сключили договор/клауза за поверителност.

8.2. Всички лични данни трябва да бъдат достъпни само за тези, които се нуждаят от тях, а достъпът може да бъде предоставен само в съответствие с изградени правила за контрол на достъпа. Всички лични данни трябва да се третират с най-голяма сигурност и трябва да се съхраняват:

- в самостоятелна стая с контролиран достъп; и/или в заключен шкаф или в картотека; и/или
- ако е компютъризирана, защитена с парола в съответствие с вътрешните изисквания посочени в организационните и технически мерки за контролиране на достъпа до информация (например правила за контрол на достъпа) ; и/или
- съхранявани на преносими компютърни носители, които са защитени в съответствие с организационните и технически мерки за контролиране на достъпа до информация.

8.3. Записите върху хартиен носител не трябва да се оставят там, където могат да бъдат достъпни от неоторизирани лица и не могат да бъдат изваждани от определените офисни помещения без изрично разрешение. Веднага щом хартиените документи вече не са необходими за текущата работа по поддръжката на клиенти, те трябва да бъдат унищожени в съответствие със създадена за това процедура/правила и съответен протокол.

8.4. Личните данни могат да бъдат изтривани или унищожавани само в съответствие с Политиката за съхраняване на личните данни. Записите на хартиен носител, които са достигнали датата на съхранение, трябва да бъдат нарязани и унищожени като "поверителни отпадъци". Данните върху твърдите дискове на излишните персонални компютри трябва да бъдат изтрити или дисковете унищожени, съгласно изградените правила/процедури.

8.5. Обработването на лични данни "извън офиса" представлява потенциално по-голям риск от загуба, кражба или нарушение на лични данни. Персоналът трябва да бъде специално упълномощен да обработва данните извън обекти на администратора.

9. Разкриване на данни

9.1. БАУКО трябва да осигури условия, при които личните данни не се разкриват на неупълномощени трети страни, което включва членове на семейството, приятели, държавни органи, дори разследващи такива, ако има основателно съмнение, че не се изискват по установения ред. Всички служители, членове на сдружението и на управителните органи на БАУКО трябва да бъдат предпазливи, когато им поискат да разкрият съхранявани лични данни за друго лице на трета страна. Важно е да се има предвид, дали разкриването на информацията е свързано или не с нуждите на дейността извършвана от организацията.

Необходимо е на служителите, членове на комисии, членове на сдружението и на управителните органи на БАУКО да се извърши специално обучение и периодични инструктажи с цел да се избегне рискът от такова нарушение.

9.2. Всички искания от трети страни за предоставяне на данни трябва да бъдат подкрепени с подходяща документация и всички такива разкривания на данни трябва да бъдат специално разрешени от определен от Председателя на УС координатор на БАУКО.

10. Съхраняване и унищожаване на данните

10.1. БАУКО не съхранява лични данни във вид, който позволява идентифицирането на субектите за по-дълъг период отколкото е необходимо, по отношение на целите, за които са били събрани данните.

10.2. БАУКО може да съхранява данни за по-дълги периоди единствено ако личните данни ще бъдат обработвани за целите на архивиране, за цели в обществен интерес, научни или исторически изследвания и за статистически цели, и само при изпълнението на подходящи технически и организационни мерки за гарантиране на правата и свободите на субекта на данните.

10.3. Периодът на съхранение за всяка категория на лични данни се уреждат от Политиката за съхранение на личните данни, както и на критериите, използвани за определяне на този период, включително всякакви законови задължения, които БАУКО е длъжно да спазва.

10.4. Политиката за съхранение на личните данни ще се прилагат във всички случаи.

10.5. Личните данни трябва да бъдат унищожени сигурно, съгласно принципа за гарантиране подходящо ниво на сигурност (чл. 5, пар. 1 б. е) от Общия регламент) – включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.

11. Трансфер на данни

Всеки трансфер на данни от рамките на ЕС към страни извън ЕС (посочени в Общия регламент като "трети страни") са незаконни, освен ако е налице подходящо "ниво на защита на основните права на субектите на данни“ или трансферът се извършва при подходящи гаранции, регламентирани от Общия регламент за защита на личните данни.

Прехвърлянето на лични данни извън ЕС е забранено, освен ако не се прилагат една или повече от указаните гаранции или изключения:

Тук трябва да се вземе предвид и съществуването на Европейско икономическо пространство. (ЕИП), което е с по-широк обхват от ЕС, и включва още страни, които не са членки на ЕС (Лихтенщайн, Норвегия и Исландия). Тези страни обаче прилагат регламенти на ЕС чрез решение на Съвместния комитет.

11.1. Решение за адекватност

Европейската комисия може да оцени трети страни, територия и/или специфични сектори в трети страни, за да прецени дали има подходящо ниво на защита на правата и свободите на физическите лица. В тези случаи не се изисква специално разрешение за трансфер на личните данни.

Комисията публикува в Официален вестник на Европейския съюз и на своя уебсайт списък на трети държави, територии и конкретни сектори в трета държава и международни организации, за които е решила, че осигуряват или че вече не осигуряват адекватно ниво на защита.

11.2. Щит за личните данни в отношенията между ЕС и САЩ (EU-U.S. Privacy Shield)

Ако БАУКО желае да прехвърли лични данни от ЕС на трета страна в САЩ, тя трябва да провери дали организацията е подписала Рамковото споразумение „Privacy Shield“ с Министерство на търговията на САЩ.

11.3. Задължителни фирмени правила

Когато е приложимо, БАУКО може да приеме одобрени задължителни корпоративни правила за прехвърляне на данни извън ЕС. Това изисква подаването им за одобрение до съответния надзорен орган.

11.4. Стандартни договорни клаузи

БАУКО може да използва утвърдени стандартни договорни клаузи за защита на данните при прехвърляне на данни извън Европейското икономическо пространство. Ако БАУКО приема стандартни договорни клаузи, одобрени от съответния надзорен орган има автоматично признаване на адекватността.

11.5. Изключения

При липса на решение за адекватност, приложимост US Privacy Shield, задължителни фирмени правила и / или договорни клаузи, прехвърляне на лични данни в трета страна или международна организация се извършва само при едно от следните условия:

- субектът на данните изрично се е съгласил с предложеното прехвърляне, след като е бил информиран за възможните рискове от такива прехвърляния;
- предаването е необходимо за изпълнението на договор между субекта на данните и администратора или за изпълнението на преддоговорни отношения, взети по искане на субекта на данните;
- предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;
- предаването е необходимо поради важни причини от обществен интерес;
- предаването е необходимо за установяването, упражняването или защитата на правни претенции;
- предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;
- предаването се извършва от регистър, който съгласно правото на ЕС или правото на държавите членки е предназначен да предоставя информация на обществеността и е достъпен за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, но само доколкото условията за справка, установени в правото на Съюза или правото на държавите членки, са изпълнени в конкретния случай.

12. Регистър на дейностите по обработване на лични данни

БАУКО прилага изключението на чл. 30, параграф 5 от Общия регламент за защита на личните данни и не поддържа регистри на дейностите по обработване на личните данни.

13. Влизане в сила и актуализация

Този документ влиза в сила от датата на утвърждаването му от Управителния съвет на БАУКО.