Hotel Expo Sofia
149, Tsarigradsko Shosse blvd.
1784 Sofia, Bulgaria
T: +359 2 817 81 00 | reservations@hotelexposofia.com
www.hotelexposofia.com

ПОЛИТИКА

ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ,

ОБРАБОТВАНИ ОТ

"САЗА ТУР" ЕООД, ЕИК: 200615942,

Утвърдена със Заповед на управителя от

10.02.2026г.

I. ЦЕЛ И ПРЕДМЕТ НА ПОЛИТИКАТА. ДЕФИНИЦИИ

Настоящата политика (по-нататък Политиката) е утвърдена в изпълнение на задълженията на "САЗА ТУР" ЕООД, ЕИК: 200615942 (по-нататък САЗА ТУР, Администратор или Дружество), опериращо хотели и извършващо съпътстващи услуги в хотелиерския бранш, както и предоставящо под наем обекти на трети лица. Действащото българско и европейско законодателство в областта на защитата на личните данни включва, но не се ограничава до Регламент (ЕС) 2016/679 относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ ЕО (по-нататък Регламентът или ОРЗД), Закона за защита на личните данни и подзаконовите актове по неговото прилагане.

1.1. Цел и предмет на Политиката

Политиката има за цел да регламентира:

1) Принципите, които се съблюдават при обработване на лични данни от „САЗА ТУР" ЕООД;

2) Поддържаните от „САЗА ТУР" ЕООД регистри на лични данни в качеството му на Администратор на лични данни;

3) Правните основания за обработване на лични данни в хода на извършване от „САЗА ТУР" ЕООД на неговата професионална и търговска дейност;

4) Целите на обработване на личните данни;

5) Категориите лични данни, които се събират и обработват;

6) Категориите субекти, чиито лични данни се събират и обработват; особени правила при някои категории субекти;

7) Категориите трети лица, на които е възможно обработваните лични данни да бъдат предоставени;

8) Лицата, които отговарят за обработването на личните данни;

9)Сроковете, за които се извършва обработването, както и процедурата за периодично проверяване на спазването на тези срокове;

10) Възприетите технически и организационни мерки и средствата за защита на обработваните от „САЗА ТУР" ЕООД лични данни, вкл. установените правила за отдалечен достъп до електронните ресурси на Дружеството;

11) Информацията, която се предоставя на субектите на данни относно правата, които имат във връзка с обработването на личните им данни, както и процедурите за упражняването на тези права;

12) Процедурите при нарушаване на сигурността на обработваните лични данни;

13) Процедурите за унищожаване на обработваните данни на хартиен и електронен носител след изтичането на сроковете за тяхното съхранение и/или отпадането на основанието за обработването им;

14) Процедурите относно извършване на периодичен преглед и актуализиране на информацията за поддържаните регистри на лични данни, вкл. на основанията за обработване и мерките за защита на личните данни.

1.2. Основни принципи при обработването

При осъществяването на всички действия, процеси и процедури, касаещи събирането и обработването на лични данни, всички служители на „САЗА ТУР" ЕООД, обработващи лични данни в хода на изпълнение на възложените им функции, следва да съблюдават спазването на следните основни принципи, заложени от Регламента:

1) Законосъобразност, добросъвестност и прозрачност - личните данни се обработват в съответствие с правните изисквания, с полагане на дължимата грижа и по начин позволяващ яснота и проследимост на обработването по отношение на субектите на данни;

2) Ограничение на целите - личните данни се събират за конкретни, изрично указани и легитимни цели и не се обработват впоследствие по начин, несъвместим с тези цели;

3) Свеждане на данните до минимум - обработват се подходящи данни, свързани с и ограничени до необходимото във връзка с целите, за които се обработват;

4) Точност - личните данни са точни; при необходимост да бъдат поддържани в актуален вид се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни;

5) Ограничение на съхранението - личните данни се съхраняват за период не по-дълъг от необходимото за целите, за които се обработват данните;

6) Цялостност и поверителност - личните данни се обработват по начин, който гарантира подходящо ниво на сигурност на данните, включително защита срещу неразрешено или незаконосъобразно обработване, случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически и организационни мерки;

7) Отчетност - спазването на горните принципи при обработването може да бъде надлежно доказано.

1.3. Дефиниции

По смисъла на настоящата Политика и в съответствие със съдържащото се в Регламента:

1) „**лични данни**“ означава 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;
2) „**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;

3) „**ограничаване на обработването**“ означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;
4) „**профилиране**“ означава 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;
5) „**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;
6) „**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;
7) „**администратор**“ означава 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;

8) „**обработващ лични данни**“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;
9) „**получател**“ означава 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;
10) „**трета страна**“ означава 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;
11) „**съгласие на субекта на данните**“ означава 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;
12) „**нарушение на сигурността на лични данни**“ означава 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;
13) „**генетични данни**“ означава лични данни, свързани с наследени или придобити генетичните белези на дадено физическо лице, които дават уникална информация за отличителните черти или здравето на това физическо лице и които са получени, по-специално, от анализ на биологична проба от въпросното физическо лице;

14) „**биометрични данни**“ означава лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни;

15) „**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.

II. ПОДДЪРЖАНИ РЕГИСТРИ НА ЛИЧНИ ДАННИ. ДОСТЪП И СЪХРАНЕНИЕ.

„САЗА ТУР" ЕООД обработва лични данни в качеството си на Администратор, в регистрите, както са посочени по-долу и подробно описани в Приложение № 1 „Регистри на дейностите по обработване в качеството на Администратор" към настоящата Политика. Информация относно:

- категориите обработвани лични данни;
- категориите физически лица, чиито данни се обработват;
- основанието и целите на обработването на личните данни;
- отговорни лица с предоставен достъп до лични данни;
- сроковете на обработване и съхранение и др.,

за всеки регистър на данни, е посочена в Приложение №1 към настоящата Политика.

2.1. Видове регистри

„САЗА ТУР" ЕООД, в качеството си на Администратор, поддържа следните регистри на лични данни:

1. Резервации;
2. Настаняване (check-in);
3. Фактуриране (контрагенти, клиенти, доставчици и гости);
4. Маркетинг;

Hotel Expo Sofia
149, Tsarigradsko Shosse blvd.
1784 Sofia, Bulgaria
T: +359 2 817 81 00 | reservations@hotelexposofia.com
www.hotelexposofia.com

5. Лоялна програма;
6. Видеонаблюдение;
7. Електронни ключове (достъп до стаи);
8. Публичен WiFi;
9. HR досиета (служители);
10. Трудова медицина;
11. Алергии и диети;
12. Жалби и рекламации;
13. Счетоводство (заплати);
14. Отзиви и оценки;
15. Уебсайт analytics и cookies;

2.2. Съхранение и достъп

Личните данни, събирани и обработвани от „САЗА ТУР" ЕООД в качеството му на Администратор, се съхраняват на електронен и/или на хартиен носител.

За различните регистри са установени различна организация на достъпа до документите, съдържащи лични данни, и различни процедури за работа с данните.

Личните данни на хартиен носител се съхраняват в отделни папки под формата на досиета в шкафове с ограничен достъп, както и в сейф, намиращи се в помещенията, ползвани от лицата, на който е възложена обработката на данните в Дружеството. Сейфът, всички шкафове и помещения се заключват.

Данните на електронен носител се съхраняват на мобилни и/или стационарни компютри и магнитни електронни носители (flash drives) на Дружеството. Помещенията, в които се намират горепосочените данни, са организирани в различни бази данни съгласно характера на личните данни, които са включени в тях. Въведена е организация на достъпа до личните данни, чрез акаунти и пароли, съответно - с различни възможности за достъп за отделните служители на Дружеството, които имат достъп до лични данни.

Достъп до обработваните и съхранявани лични данни на хартиен и/или електронен носител имат само и единствено лицата, посочени в графата "Получатели" за всеки отделен Регистър, съгласно Приложение № 1 към настоящата Политика.

Hotel Expo Sofia
149, Tsarigradsko Shosse blvd.
1784 Sofia, Bulgaria
T: +359 2 817 81 00 | reservations@hotelexposofia.com
www.hotelexposofia.com

При осъществяването на достъпа до личните данни от съответния регистър се спазват установените за регистъра технически и организационни мерки, както са описани в раздел III от настоящата Политика и в Приложение № 1 към нея.

Сроковете за съхранение на личните данни в отделните регистри са различни с оглед на различните основания и цели на обработването им-посочени в Приложение №1.

2.3 Облачно съхранение на лични данни. Специални правила за мерки за защита при облачно съхранение.

„САЗА ТУР" ЕООД може , но не е задължен, да използва и облачни услуги за съхранение и обработка на лични данни с цел:

• Осигуряване на достъпност на данните от различни локации;

• Автоматично създаване на резервни копия;

•Защита срещу физическа загуба на данни (пожар, наводнение, кражба на устройства);

• Улесняване на съвместната работа на служителите;

• Съответствие със съвременните бизнес практики.

Дружеството може да използва следните категории облачни услуги:

А) ОБЛАЧНО СЪХРАНЕНИЕ НА ФАЙЛОВЕ

Услуги: Google Drive, Microsoft OneDrive, Dropbox, iCloud и подобни

Обработвани данни:

• Договори с гости и доставчици (сканирани копия);

• Счетоводни документи и фактури;

• Вътрешни документи и политики;

• HR досиета на служители.

Мерки за защита:

• Използване само на бизнес/корпоративни версии (не безплатни лични акаунти);

• Двуфакторна автентикация (2FA) задължително за всички потребители;

• Криптиране на чувствителни файлове преди качване (при необходимост);

• Регулярен одит на споделени папки и връзки;

• Ограничаване на външно споделяне;

• Конфигуриране на автоматично изтриване на файлове от кошчето след определен период.

Б) ОБЛАЧНИ РЕЗЕРВАЦИОННИ СИСТЕМИ

Услуги: Booking.com и подобни

Обработвани данни:

• Имена и контакти на гости;

• Данни за кредитни карти (токенизирани);

• История на резервации;

• Преференции на гости;

• Рейтинги и отзиви.

Мерки за защита:

• Договор по чл. 28 от GDPR с доставчика на системата;

• Силни пароли и двуфакторна автентикация;

• Ограничаване на достъпа по IP адрес (където е възможно);

• Логове на всички действия в системата;

• Редовно изтегляне на локални резервни копия;

• Изтриване на данни след изтичане на законовите срокове.

В) ОБЛАЧНА ИМЕЙЛ ПЛАТФОРМА

Услуги: Gmail (Google Workspace), Outlook (Microsoft 365), и подобни

Обработвани данни:

• Кореспонденция с гости (резервации, потвърждения, рекламации);

• Комуникация с доставчици и партньори;

• Вътрешна кореспонденция със служители;

• Прикачени файлове с лични данни.

Мерки за защита:

• Бизнес версия на имейл услугата (с административен контрол);

• Двуфакторна автентикация задължително;

• Автоматично изтриване на имейли в кошчето след 30 дни;

• Филтри за предотвратяване на фишинг атаки;

• Обучение на служителите как да разпознават измамни имейли;

• Забрана за препращане на имейли с лични данни към лични адреси;

• Автоматично архивиране според политиката за съхранение.

Г) ОБЛАЧЕН СЧЕТОВОДЕН СОФТУЕР

Услуги: Счетоводни системи

Обработвани данни:

• ЕГН/ЛНЧ на служители;

• Данни за заплати и осигуровки;

• Фактурни данни на гости и доставчици;

• IBAN, банкови сметки;

• Данъчни декларации.

Мерки за защита:

• Договор с доставчика по чл. 28 от GDPR;

• Потвърждение, че данните се съхраняват в ЕИП;

• Многофакторна автентикация;

• Достъп само за упълномощени лица (счетоводител, управител);

• Редовни одити на потребителските права;

• Криптирано свързване (SSL/TLS).

Д) ОБЛАЧНИ CRM СИСТЕМИ

Услуги: CRM платформи за управление на клиентски взаимоотношения

Обработвани данни:

• Контакти на гости и потенциални клиенти;

• История на комуникацията;

• Преференции и забележки;

• Маркетингови съгласия.

Мерки за защита:

• Договор по чл. 28 от GDPR;

• Двуфакторна автентикация;

• Поддържане на актуален списък с лица с достъп;

• Автоматично сегментиране на контакти според маркетингови съгласия;

• Възможност за бърз експорт и изтриване на данни.

При избор на доставчик на облачни услуги, Дружеството проверява:

✓ Наличие на сертификати ISO 27001, SOC 2 или подобни стандарти за сигурност;

✓ Локация на дата центровете (предпочитание за ЕИП);

✓ Готовност за сключване на договор по чл. 28 от GDPR;

✓ Прилагани мерки за криптиране (в покой и при пренос);

✓ Политики за резервни копия и възстановяване при бедствия;

✓ Процедури при прекратяване на услугата (експорт и изтриване на данни);

✓ Време за реакция при инциденти със сигурността;

✓ SLA (Service Level Agreement) - гаранции за достъпност.

Договори с доставчици на облачни услуги

Със всеки доставчик на облачни услуги, обработващ лични данни от името на „САЗА ТУР" ЕООД, се сключва писмен договор (или се приемат Стандартни договорни клаузи), който съдържа:

• Предмет, продължителност, естество и цел на обработването;

• Вид лични данни и категории субекти;

• Задължения и права на администратора;

• Задължения на обработващия (обработва данните само по инструкции, гарантира поверителност, прилага мерки за сигурност);

• Подизпълнители - право на администратора да одобрява подизпълнители;

• Помощ на администратора при упражняване на права на субектите;

• Помощ при осигуряване на сигурност и уведомяване при инциденти;

• Изтриване или връщане на данните след прекратяване;

• Право на одит и проверки;

• Специфични гаранции съгласно чл. 28 от GDPR.

2.4 Мобилни устройства и отдалечен достъп

Използване на мобилни устройства

Hotel Expo Sofia
149, Tsarigradsko Shosse blvd.
1784 Sofia, Bulgaria
T: +359 2 817 81 00 | reservations@hotelexposofia.com
www.hotelexposofia.com

Служителите на „САЗА ТУР" ЕООД могат да използват мобилни устройства (смартфони, таблети, лаптопи) за достъп до лични данни при следните условия:

СЛУЖЕБНИ УСТРОЙСТВА:

• Устройствата са собственост на Дружеството;

• Конфигурирани са от IT администратор/Координатор по защита на данните;

• Имат активирано криптиране на диска;

• Защитени са с PIN/парола/биометрия;

• Инсталиран е антивирусен софтуер;

• Настроено е автоматично заключване след 5 минути неактивност;

• Възможност за дистанционно изтриване при загуба/кражба (MDM - Mobile Device Management);

• Забранени са root/jailbreak модификации.

ЛИЧНИ УСТРОЙСТВА (BYOD - Bring Your Own Device):

Ако се разрешава използването на лични устройства:

• Служителят подписва декларация за спазване на политиката за сигурност;

• Достъпът е само до строго ограничени данни (напр. имейл, календар);

• Двуфакторна автентикация задължително;

• Забрана за съхранение на локални копия на файлове с лични данни;

• Незабавно уведомяване при загуба или кражба на устройството;

• Право на Дружеството да изиска изтриване на служебни данни при прекратяване.

2.5 Отдалечен достъп и работа от разстояние

При необходимост от отдалечен достъп (работа от дома, служебни пътувания):

ТЕХНИЧЕСКИ МЕРКИ:

• VPN (Virtual Private Network) за сигурна връзка към корпоративната мрежа;

• Многофакторна автентикация;

• Достъп само до необходимите системи и данни;

• Забрана за използване на публични WiFi мрежи без VPN;

• Криптирани комуникации (HTTPS, SSL/TLS);

• Автоматично прекъсване на връзката при неактивност.

ОРГАНИЗАЦИОННИ МЕРКИ:

• Писмено разрешение от ръководство за отдалечен достъп;

• Обучение на служителите за рисковете при отдалечена работа;

• Забрана за споделяне на достъп с членове на семейството;

• Осигуряване на физическа поверителност (екранът да не е видим от трети лица);

• Документиране на часовете на отдалечен достъп (в логовете на системата).

2.6 Политика за пароли и автентикация

Всички служители, имащи достъп до лични данни, трябва да спазват следните правила:

ИЗИСКВАНИЯ КЪМ ПАРОЛИТЕ:

• Минимална дължина: 12 символа;

• Комбинация от главни и малки букви, цифри и специални символи;

• Различни пароли за различни системи (забрана за преизползване);

• Смяна на паролата при подозрение за компрометиране;

• Използване на парол мениджър (препоръчително);

• Забрана за записване на пароли на видими места или в незащитени файлове.

МНОГОФАКТОРНА АВТЕНТИКАЦИЯ (MFA/2FA):

Задължително за:

• Имейл акаунти;

• Облачни системи за съхранение;

• Административен достъп до резервационни системи;

• Достъп до счетоводен софтуер;

• Видеонаблюдение и облачно съхранение на видеозаписи.

2.7 Забрани при използване на устройства

СТРОГО ЗАБРАНЕНО е:

✗ Изпращане на имейли с лични данни към лични адреси;

✗ Качване на файлове с лични данни в лични облачни акаунти;

✗ Използване на неоторизиран софтуер или приложения;

✗ Свързване на служебни устройства към недоверени мрежи без защита;

✗ Оставяне на отключени устройства без надзор;

✗ Споделяне на пароли между служители;

✗ Разпечатване на документи с лични данни на обществени принтери;

✗Дискутиране на лични данни на гости на обществени места.

2.8 Политика за резервни копия (Backup)

„САЗА ТУР" ЕООД създава редовни резервни копия на всички критични данни за да осигури:

• Защита срещу случайна загуба или изтриване;

• Възможност за възстановяване при хардуерна повреда;

• Защита при атаки или злонамерени действия;

• Съответствие с принципа за цялостност и наличност на данните.

ЧЕСТОТА НА РЕЗЕРВНИТЕ КОПИЯ:

• Критични данни (резервации, фактури) - ежедневно;

• Счетоводни данни - ежедневно;

• HR досиета и договори - седмично;

• Видеонаблюдение - автоматично в облака (при текущо съхранение);

• Архивни данни - месечно.

ЛОКАЦИЯ НА РЕЗЕРВНИТЕ КОПИЯ:

• Първично резервно копие - на облачна платформа (различна от основното хранилище);

• Вторично резервно копие - на локален външен твърд диск (за критични данни);

• Офсайт копие - съхранено физически на друга локация (ако е приложимо).

Правило 3-2-1:

• 3 копия на данните (оригинал + 2 резервни);

• 2 различни носителя (напр. облак + локален диск);

• 1 копие на отдалечено място.

2.9. Специални сценарии и рискове

- ✓ Работа с платежни данни

При обработка на данни за кредитни/дебитни карти:

• Дружеството НЕ съхранява пълни номера на карти (само последните 4 цифри за справка);

• Използване на токенизация - платежният процесор заменя номера на картата с токен;

• Строг контрол кой има достъп до платежния терминал;

• Забрана за записване на CVV кода;

• Криптирани връзки при онлайн плащания (SSL/TLS).

- ✓ Скенери и копирни машини

Многофункционални устройства (принтер/скенер/копир):

• Изтриване на кеш паметта на устройството редовно;

• Защита с парола на функцията за сканиране към имейл;

• Забрана за съхранение на документи на твърдия диск на устройството;

• Незабавно вземане на разпечатани документи (без оставяне в принтера);

• При извеждане от употреба - пълно изтриване на паметта.

- ✓ Видеоконферентни платформи

При използване на Zoom, Teams, Google Meet и подобни:

• Активиране на чакалня (waiting room) за контрол на участниците;

• Парола за достъп до срещи с чувствителни теми;

• Деактивиране на автоматичното записване;

• Ако се прави запис - изрично съгласие от участниците;

• Изтриване на записи след изпълнение на целта;

• Забрана за публикуване на линкове за срещи в публични канали.

- ✓ Социални мрежи и маркетинг

При публикуване на снимки/видео от хотела:

• Получаване на писмено съгласие от гостите преди публикуване;

• Избягване на снимки със ясно видими лица (или замъгляване);

• Незабавно изтриване при искане от субекта;

• Отделна политика за cookies на уебсайта;

• Прозрачност относно използването на пиксели за проследяване (Facebook Pixel, Google Analytics).

2.10. Видеонаблюдение и обработване на видеозаписи

Правно основание и цели на видеонаблюдението

„САЗА ТУР" ЕООД може да осъществява видеонаблюдение на определени зони в хотелските си обекти на основание чл. 6, пар. 1, буква (е) и (ж) от Регламента, а именно:

1) Изпълнение на задача от обществен интерес - осигуряване на безопасността на гостите, служителите и посетителите;

2) Защита на законните интереси на Администратора, включително:

- Предотвратяване и разкриване на престъпления;
- Защита на имуществото на Дружеството и гостите;
- Осигуряване на обществения ред и безопасност в хотелските обекти;
- Опазване на здравето и безопасността на гости и персонал;
- Доказване на факти при евентуални правни спорове.

Обхват на видеонаблюдението

Видеонаблюдение се осъществява в следните зони:

1) Общи части - входове, фоайета, коридори, паркинги, външна територия;

2) Работни зони - рецепция, складови помещения, технически помещения;

3)Обществени пространства - ресторанти, барове, конферентни зали (при необходимост).

ВАЖНО: Видеонаблюдение НЕ се осъществява в:

- Хотелски стаи и апартаменти;
- Санитарни помещения и тоалетни;
- Фитнес зали и спа центрове (освен входове);
- Гардеробни на персонала;
- Други зони, където съществува разумно очакване за неприкосновеност на личния живот.

Технически параметри

Използваните системи за видеонаблюдение съответстват на следните технически изисквания:

1) Камерите са насочени така, че да заснемат минимално необходимата зона за постигане целите на наблюдението;

2) Резолюцията на записите е достатъчна за постигане на целите, но не по-висока от необходимото;

3) Видеозаписите се съхраняват криптирано на облачна платформа с високи стандарти за сигурност;

4) Достъпът до облачната платформа е защитен с многофакторна автентикация;

5) Системата поддържа логове за всички достъпи до видеозаписи.

Облачно съхранение на видеозаписи

Видеозаписите от системата за видеонаблюдение се съхраняват на облачна платформа, предоставена от доставчик на облачни услуги, който действа като Обработващ лични данни.

1) С доставчика на облачни услуги е сключен договор по чл. 28 от Регламента, който гарантира:

- Съответствие със стандартите за сигурност на информацията;
- Съхранение на данните в дата центрове в рамките на ЕИП;
- Криптиране на данните при пренос и в състояние на покой;
- Редовно създаване на резервни копия;
- Възможност за изтриване на данни при изтичане на срока за съхранение.

2) Доставчикът на облачни услуги се задължава да:

- Обработва данните само по документирани инструкции от Администратора;
- Не предоставя достъп до данните на трети лица без изричното съгласие на Администратора;
- Уведомява незабавно Администратора при инциденти със сигурността;
- Предоставя на Администратора информация за прилаганите мерки за защита.

Срок за съхранение на видеозаписи

Видеозаписите се съхраняват за период от 30 (тридесет) календарни дни, след което автоматично се изтриват от системата, освен когато:

1) Записът е необходим за установяване, упражняване или защита на правни претенции;

2) Записът е поискан от компетентни органи (полиция, прокуратура, съд);

3) Записът документира инцидент, който изисква по-дълго съхранение.

При наличие на някое от горните основания, видеозаписът се съхранява в отделна защитена папка за необходимия период, но не по-дълго от:

- 5 (пет) години при установяване на престъпление;
- 3 (три) години при гражданскоправни спорове;
- Докато не отпадне необходимостта, ако е поискан от компетентни органи.

Достъп до видеозаписи

Достъп до видеозаписите от системата за видеонаблюдение имат само упълномощени служители, определени със Заповед на Управителя, включващи:

1) Управител на Дружеството;

2) Технически отговорник за видеонаблюдението;

3) Мениджър на хотелския обект.

Всички служители с достъп до видеозаписите са задължени:

- Да пазят в тайна всякаква информация, получена при преглед на записите;
- Да не правят неразрешени копия на записи;
- Да докладват незабавно на Управителя всякакви подозрителни опити за достъп;
- Да използват записите само за легитимни и документирани цели.

Всеки достъп до видеозаписи се документира и включва:

- Дата и час на достъпа;
- Лице, извършило достъпа;
- Цел на преглед на записа;
- Информация за конкретния запис, който е прегледан.

Информиране на субектите на данни

„САЗА ТУР" ЕООД информира субектите на данни за наличието на видеонаблюдение чрез:

1) Поставяне на ясно видими информационни табели на входа на всяка видеонаблюдавана зона, съдържащи:

- Информация, че зоната е под видеонаблюдение;
- Наименование и контакти на Администратора;
- Цел на видеонаблюдението;
- Правното основание за обработване;

- Срок за съхранение на записите;
- Права на субектите на данни;

2) Публикуване на информация на рецепцията и в общодостъпни места в хотела;

3) Включване на информация за видеонаблюдението в общите условия при настаняване.

Предоставяне на видеозаписи на трети лица

Видеозаписи могат да бъдат предоставени на трети лица само в следните случаи:

1) При наличие на законово задължение - по искане на органи на Министерството на вътрешните работи, прокуратурата, съда или други компетентни държавни органи;

2) При необходимост за защита на законни интереси - при инциденти, застрахователни претенции или правни спорове, но само в обема, необходим за конкретния случай;

3) При изрично съгласие на засегнатите субекти на данни.

При всяко предоставяне на видеозапис се съставя писмен протокол, който се съхранява заедно с копие от искането/заповедта за предоставяне.

Права на субектите относно видеонаблюдението

Субектите на данни имат право:

1) Да получават информация дали съществуват видеозаписи, на които са заснети;

2) Да получават достъп до видеозаписи, на които са идентифицируеми;

3) Да искат изтриване на записи при определени условия;

4) Да възразят срещу обработването при наличие на особени обстоятелства;

5) Да подадат жалба до Комисията за защита на личните данни.

При упражняване на правата си, субектите следва да подадат писмено искане, съдържащо достатъчно информация за идентифициране на конкретния видеозапис (дата, час, локация).

III. СЪГЛАСИЕТО КАТО ОСНОВАНИЕ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

При необходимост и когато това е допустимо от Регламента и действащото законодателство, Дружеството обработва лични данни като Администратор и въз основа на изрично писмено съгласие на субекта на данните за такова обработване.

Когато обработва лични данни въз основа на съгласие от субектите на данни, Дружеството гарантира, че съгласието е дадено и че то отговаря на изискванията на Общия регламент за защита на данните (ОРЗД), а именно:

- съгласието е ясно разграничимо, когато е част от друг документ;
- съгласието съдържа ясна и недвусмислена информация относно целите и сроковете за обработване на личните данни;
- предоставена е възможност на субектите да дадат отделно съгласие за различните цели на обработване;
- лицата са информирани за възможността да оттеглят съгласието си по всяко време и им е осигурен лесен начин за това;
- изпълнението на договор/ предоставянето на услуга не е поставено в зависимост от предоставянето на съгласието за обработване, когато последното не е необходимо за изпълнението на договора/ предоставянето на услугата.

При оттегляне на съгласието, събраните лични данни се унищожават в съответствие с правилата и изискванията на настоящата Политика, освен ако „САЗА ТУР" ЕООД не прецени, че е налице легитимен интерес или е възникнало законово задължение данните да бъдат съхранени за определен срок. Оттеглянето на съгласието от субекта на данни не засяга законосъобразното обработване на данни, извършено до момента на това оттегляне.

IV. ОТНОШЕНИЯ МЕЖДУ АДМИНИСТРАТОРА И ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

В случаите, когато Дружеството, в качеството му на Администратор, възлага обработването на определени лични данни на трето лице -обработващ данните, отношенията с обработващия се регламентират от писмен акт (договор), който детайлизира задълженията на обработващия в съответствие с Регламента и

Hotel Expo Sofia
149, Tsarigradsko Shosse blvd.
1784 Sofia, Bulgaria
T: +359 2 817 81 00 | reservations@hotelexposofia.com
www.hotelexposofia.com

относимото национално законодателство, вкл. прилагането от последния на подходящи технически и организационни мерки за защита на обработваните лични данни. Преди сключването на договора Дружеството проучва третото лице, на което евентуално ще бъде възложено обработването на данни, с цел да се увери, че това трето лице разполага с необходимите експертни знания, надеждност и ресурси, и при възлагането на такова обработване ще бъдат налице достатъчно гаранции за защитата на правата на субектите на лични данни и за тяхното законосъобразно обработване.

За тази цел Координаторът по защита на данните предприема и документира извършването на следните действия: 1) проверява репутацията на обработващия посредством общодостъпните източници на информация; 2) изисква информация за вътрешните актове относно защита на данните, приети от обработващия и доказателства, за начина, по който служителите на обработващия са ангажирани с тяхното спазване; и 3) изисква информация за използвания софтуер за обработка на данните, както и за въведените други технически и организационни мерки за защита на данните.

Координаторът по защита на данните следи писменият акт (договора) между Дружеството и обработващия да отговаря на специфичните изисквания на Регламента.

V. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Личните данни, събирани и обработвани от „САЗА ТУР" ЕООД в качеството му на Администратор е възможно да бъдат предоставени на следните (категории) лица:

Личните данни, обработвани от „САЗА ТУР" ЕООД могат да бъдат предоставени на следните категории получатели:

1) на компетентните органи -- напр. Национален осигурителен институт, Национална агенция за приходите, Изпълнителна агенция „Главна инспекция по труда", Държавна агенция „Национална сигурност", Министерство на вътрешните работи, Комисията за защита на личните данни, Търговски регистър, органите на съда, прокуратурата и Министерство на вътрешните работи и др.

2) Правни, данъчни и други консултанти и одитори;

3) Доставчици на IT услуги; софтуерни компании;

4) Доставчици на счетоводни услуги и други услуги, свързани с дейността на дружеството -агенции за набиране на персонал, туроператори, пътнически компании, контрагенти на „САЗА ТУР" ЕООД, за изпълнение на договорите, с които се командироват служители на „САЗА ТУР" ЕООД, дружества, извършващи обучения и др.;

5) Други дружества от групата на едноличния собственик на капитала на „САЗА ТУР" ЕООД;

Лични данни от Регистър Персонал се предоставят за обработване и на:

1) службата по трудова медицина;

2) застрахователни дружества във връзка с допълнително задължително здравно застраховане на територията на Р.България;

3) банкови институции;

4) доставчик на туроператорски услуги;

5) доставчик на обучителни услуги;

6) външни HR компании;

7) външни софтуерни компании, доставчици на софтуерни услуги и електронни трудови досиета;

VI. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ ИЗВЪН ЕИП

„САЗА ТУР" ЕООД не планира да предоставя лични данни на трети лица извън границите на Европейското икономическо пространство (ЕИП). Изключение евентуално би било единствено предаване на лични данни към работодатели на гостите на хотелите, които са със седалище извън ЕИП или при ползване на облачни услуги и дата центрове при наличие на строги механизми за защита (като Стандартни договорни клаузи - SCCs или Data Privacy Framework).Всеки трансфер се регистрира и се извършва само след правна проверка и документиране и при стриктно спазване на глава V от Регламента.

Hotel Expo Sofia
149, Tsarigradsko Shosse blvd.
1784 Sofia, Bulgaria
T: +359 2 817 81 00 | reservations@hotelexposofia.com
www.hotelexposofia.com

VII. ПРОЦЕДУРА ЗА АКТУАЛИЗИРАНЕ НА ИНФОРМАЦИЯТА ПО РЕГИСТРИ

При необходимост, но не по-рядко от веднъж годишно, в срок до 31 декември на съответната година, служителите на „САЗА ТУР" ЕООД, на които е възложено обработването на събраните лични данни, проверяват дали е настъпила някаква фактическа промяна в дейностите по обработка, отразени в регистрите по Приложение № 1 (вкл. в основанията, целите, обработваните данни, субектите, получателите, и т.н.) и дали не се налага такава промяна поради законодателни изменения или други съображения.

Резултатите от проведената проверка се документират посредством писмен протокол, съдържащ констатации и препоръки за действие. В случай, че е констатирана необходимост от въвеждането на промени в регламентацията на дейностите по обработка в регистрите, се предприемат действия по приемане на съответни промени в настоящата Политика.

VIII. ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА

8.1. Общи принципи при въвеждането на мерки за защита

В качеството си на Администратор на лични данни, „САЗА ТУР" ЕООД извършва периодична оценка на рисковете за правата на лицата, свързани с обработваните от него лични данни, и въвежда и прилага подходящи технически и организационни мерки, за да гарантира, че е в състояние да осигури законосъобразното обработване на личните данни на основанията и за целите, за които то се извършва, включително - че по подразбиране данните не са достъпни за неограничен брой физически лица (защита на данните по подразбиране).

При избор, внедряване и/или имплементиране на нови софтуерни продукти, конфигурации и системи, имащи отношение към обработката на лични данни, Дружеството, отчитайки достиженията на техническия прогрес, разходите за прилагането на новите софтуерни продукти, конфигурации и системи, както и рисковете от обработването на данните за правата на лицата, взема предвид, че те следва допълнително да гарантират още на етапа на проектиране (защита на данните на етапа на проектиране), че:

Hotel Expo Sofia
149, Tsarigradsko Shosse blvd.
1784 Sofia, Bulgaria
T: +359 2 817 81 00 | reservations@hotelexposofia.com
www.hotelexposofia.com

- обработваните лични данни са сведени до минимум -обработват се само лични данни, които е необходимо да се обработват за заявените цели;
- личните данни са достъпни само за необходимия кръг лица с оглед на заявените цели на обработване;
- е налице прозрачност по отношение на функциите и обработването на личните данни;
- че се използват приложения и процеси, които позволяват въвеждането на подходящи мерки за защита на данните.

8.2. Видове прилагани мерки за защита

По отношение на личните данни, събирани и обработвани от Дружеството, в качеството му на Администратор, са приети и въведени в изпълнение следните технически и организационни мерки за защита на личните данни:

1) Физическа защита на личните данни, която се осъществява посредством:

- Съхраняване на личните данни на хартиен носител в сейф и в шкафове с ключалки, разположени в заключващи се помещения;
- Ограничен достъп до помещенията, в които се съхраняват лични данни;
- Офис помещенията се заключват;

2) Електронен подпис - на Координатора по защита на данните, по негова преценка;

3) Логическа защита относно личните данни, съхранявани на електронен носител - Firewall (FW), Antivirus (AV);

4) Логическа защита относно личните данни, съхранявани на електронен носител, намиращи се на работните станции (персонални компютри) на отделните служители, на които е възложено практическото обработване на личните данни;

5) Контролиран достъп до личните данни, съхранявани и обработвани на електронен носител въз основа на следните критерии -предварително зададено ниво на достъп, потребителско име и парола за достъп;

6) Водене на записи (логове) най-малко за следните операции по обработването: събиране, промяна, справки, разкриване, включително предаване, комбиниране и изтриване, което дава възможност за установяване на основанието, датата и часа на такива операции и доколкото е възможно -идентификацията на лицето, което е

Hotel Expo Sofia
149, Tsarigradsko Shosse blvd.
1784 Sofia, Bulgaria
T: +359 2 817 81 00 | reservations@hotelexposofia.com
www.hotelexposofia.com

направило справка или е разкрило лични данни, както и данни, идентифициращи получателите на тези лични данни, в обема и вида, в който тези записи се поддържат от програмните продукти, с които работят служителите на Дружеството.

7) Подсигуряване на спазването на поетите задължения за конфиденциалност, посредством поемане на задължения от обработващите лични данни, както и от служителите и изпълнителите по граждански договори, работещи в Дружеството, чрез предвиждането им в сключените с тях договори или прилежащите им документи, както и възлагане на задължения във връзка с обработването на лични данни, поемане на ангажимент за поверителност в длъжностната характеристика на служителите, на които е възложено обработване на лични данни и задължение за спазване на Политиката за защита на личните данни;

8) Архивиране и инвентаризиране на документите на хартиен носител, от посочените по-горе регистри, съдържащи лични данни, както и ограничаване на достъпа до така архивираните данни само до оторизирани за това лица, съгласно правилата на настоящата Политика и Приложение № 1 към нея;

9) Периодично архивиране на личните данни, съхранявани на електронен носител.

8.3. Процедура за проверка по спазването на прилаганите мерки за защита. Актуализиране на мерките.

С оглед минимизиране на рисковете, които са свързани с обработването налични данни, и по-конкретно - от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до обработвани лични данни, Дружеството извършва периодично изпитване, преценка и оценка на ефективността на прилаганите технически и организационни мерки.

При извършването на тази преценка се проверява на извадков принцип и фактическото спазване на установените в настоящата Политика мерки от лицата, обработващи лични данни в регистрите съгласно Приложение № 1.

Проверката относно прилагането на мерките и преценката за тяхната ефективност и актуалност се извършват периодично, но не по-рядко от веднъж годишно, в срок до 31 декември на съответната година, от Координатора по защита на данните.

Резултатите от проведената проверка се документират посредством отчет и/или протокол, съдържащ констатации и препоръки. В случай, че е констатирана необходимост от въвеждането на нови мерки за защита, се предприемат съответни промени в настоящата Политика

IX. СПЕЦИАЛНИ ПРАВИЛА ПРИ ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чувствителни лични данни

9.1. Основания за обработване на чувствителни лични данни

Събирането и обработването на специални категории лични данни (чувствителни данни) като правило се извършва от „САЗА ТУР" ЕООД, в качеството му на Администратор, когато това е необходимо за целите на изпълнението на задълженията и упражняването на специалните права на Дружеството или на субекта на данните по силата на трудовото право (чрез софтуер за обработката на възнагражденията и поддържането на трудовите досиета на служителите на Дружеството, въз основа на договор с трето-лице обработващ данните), за целите на превантивната или трудовата медицина (чрез възлагане на Служба по трудова медицина, обвързана от задължение по закон за спазване на поверителност) или в други, изрично допустими от Регламента и/ или действащото законодателство случаи.

9.2. Допълнителни мерки за защита при обработване на чувствителни лични данни

При обработването на чувствителни лични данни „САЗА ТУР" ЕООД осигурява прилагането на по-строги мерки за тяхната защита (включително при получаване/ предаване на информацията и при последващото ѝ обработване и съхранение) с оглед осигуряването на подходящи гаранции за правата на субектите на данни.

При автоматизираното обработване на чувствителни данни „САЗА ТУР" ЕООД, в качеството си на Администратор на лични данни, след извършена оценка на рисковете за правата на субектите на данни, прилага мерки, имащи за цел осигуряване на:

1) контрол върху носителите на данни (да се предотврати четенето, копирането, изменянето или отстраняването на носители на данни от неоправомощени лица);

2) контрол върху съхраняването (да се предотврати въвеждането на лични данни, изменянето или заличаването на съхранявани лични данни от неоправомощени лица, както и извършването на проверки в тази връзка);

3) контрол върху потребителите (да се предотврати използването на информационната система на Дружеството от неоправомощени лица чрез използване на оборудване за предаване на данни);

4) контрол върху достъпа до данни (да се гарантира, че лицата, на които е разрешено да използват информационната система на Дружеството, имат достъп само до личните данни, които са обхванати от тяхното разрешение за достъп);

5) контрол върху комуникацията (да се гарантира възможността за проверка и установяване на кои служители/ органи са били или могат да бъдат предадени данни или имат достъп до лични данни чрез оборудване за предаване на данни);

6) контрол върху въвеждането на данни (да се гарантира възможността за последваща проверка и установяване на това какви лични данни са били въведени в информационната система на Дружеството, както и кога и от кого са били въведени тези лични данни);

7) контрол върху пренасянето (да се предотврати четенето, копирането, изменянето или заличаването на лични данни от неоправомощени лица при предаването на лични данни или при пренасянето на носители на данни);

8) възстановяване (да се гарантира възможността за възстановяване на инсталираните системи в случай на отказ на функциите на системите);

9) надеждност (да се гарантира изпълнението на функциите на информационната система и докладването за появили се във функциите дефекти);

10) цялостност (да се гарантира недопускане на увреждане на съхраняваните лични данни вследствие на неправилно функциониране на информационната система).

По-конкретно, в допълнение към мерките за защита, „САЗА ТУР" ЕООД прилага и следните мерки:

- Във всички случаи на предаване/ прехвърляне на информацията по електронен път и/или на електронен носител, личните данни се защитават посредством криптиране на информацията в началната точка на предаване/ прехвърляне и декриптирането ѝ

в крайната точка, включително чрез използване на парола, криптираща програма или електронен подпис.

- Достъп до съхраняваните чувствителни лични данни осъществяват само лицата с предоставен достъп, съгласно правилата на тази Политика и Приложение № 1 към нея.

Данни на хотелски гости

9.3 Видове обработвани данни

В хода на предоставяне на хотелиерски услуги, „САЗА ТУР" ЕООД обработва следните категории лични данни на гости:

1) Резервационни данни:

- Имена (собствено и фамилно);
- Телефон и електронна поща;
- Предпочитания относно тип стая;
- Специални изисквания (евентуално алергии, достъпност и др.);
- Данни за плащане (номер на карта - криптиран);

2) Данни при настаняване:

- Документ за самоличност (данни от него)- не се прави копие на документ за самоличност!
- Адрес на постоянно пребиваване;
- Гражданство;
- Дата на раждане;
- Данни за съпътстващи лица;
- Номер на МПС (при ползване на паркинг);

3) Данни за престоя:

- Дати на настаняване и напускане;
- Номер на стая;
- Ползвани допълнителни услуги;
- Фактурни данни (при поискване на фактура);
- Преференции и забележки.

9.4. Правни основания за обработване

Hotel Expo Sofia
149, Tsarigradsko Shosse blvd.
1784 Sofia, Bulgaria
T: +359 2 817 81 00 | reservations@hotelexposofia.com
www.hotelexposofia.com

Обработването на личните данни на хотелските гости се извършва на следните правни основания:

1) Изпълнение на договор (чл. 6, пар. 1, буква б) от Регламента) - данните са необходими за сключване и изпълнение на договора за настаняване;

2) Изпълнение на законово задължение (чл. 6, пар. 1, буква в) от Регламента):

- Водене на регистър на чужденците по Закона за чужденците в РБ;
- Издаване на фактури и счетоводно отчитане съгласно ЗДДС и ЗСч;
- Съхранение на данни за данъчни цели;

3) Законен интерес на Администратора (чл. 6, пар. 1, буква е) от Регламента):

- Управление на резервации и предотвратяване на неявяване;
- Обработка на рекламации и подобряване на услугите;
- Директен маркетинг (при наличие на съгласие или легитимен интерес);
- Предотвратяване на измами и кражби, за защита на имущество и безопасност.

9.5. Срокове за съхранение

Личните данни на хотелските гости се съхраняват за следните срокове:

1) Резервационни данни (при отменена резервация) - 1 (една) година;

2) Данни от регистъра на настанените лица - 5 (пет) години (по Закона за чужденците);

3) Фактурни данни - 10 (десет) години (по Закона за счетоводството);

4) Маркетингови данни - до оттегляне на съгласието или 3 (три) години от последния контакт;

5) Данни за рекламации - 5 (пет) години от приключване на процедурата.

Данни на служители

9.6 Специфики при хотелската дейност

При обработване на данни на служители в хотелската индустрия, „САЗА ТУР" ЕООД взема предвид спецификите на работата на смени, достъпа до лични данни на гости и необходимостта от повишена сигурност.

9.7. Допълнителни категории данни

Освен стандартните данни на служители (трудов договор, осигуровки и др.), Дружеството може да обработва:

Hotel Expo Sofia
149, Tsarigradsko Shosse blvd.
1784 Sofia, Bulgaria
T: +359 2 817 81 00 | reservations@hotelexposofia.com
www.hotelexposofia.com

1) Данни за проверка на минало - при позиции, изискващи достъп до имущество или лични данни на гости;

2) Данни от видеонаблюдение - за защита на имуществото и безопасност;

3) Данни за обучения - специфични обучения по работа с гости, GDPR, и др.;

4) Данни за работно облекло и екипировка - за хотелски униформи и оборудване.

9.8. Достъп до системи

Служителите получават достъп само до тези системи и данни, които са необходими за изпълнение на трудовите им задължения:

1) Рецепционисти - достъп до резервационна система и данни на гости;

2) Управление - достъп до финансови и организационни данни;

3) Технически персонал - достъп до видеонаблюдение (при необходимост);

4) Хотелиерско обслужване - ограничен достъп само до номера на стаи и имена.

9.9.Обработване на лични данни на непълнолетни (под 18 години)

Непълнолетните лица (деца и юноши под 18 години) се ползват със специална защита при обработване на техните лични данни съгласно GDPR.

• Резервация и настаняване на деца се прави от родител/настойник;

• Детето НЕ дава собствено съгласие за обработване - родителят го прави;

• Директен маркетинг към деца - ЗАБРАНЕН

ОБРАБОТВАНИ ДАННИ:

• Име на детето

• Възраст/дата на раждане

• Гражданство (при чужденци - за регистър)

• Специални изисквания (детско креватче, високо столче)

• Алергии (ако родителят доброволно предостави)

НАСТАНЯВАНЕ НА НЕПЪЛНОЛЕТЕН БЕЗ РОДИТЕЛ (рядко)

ГРУПИ ОТ ДЕЦА (училищни екскурзии, спортни лагери)

ОБРАБОТВАНЕ:

• Списък с имената на децата

• Контакти на родители/настойници

• Медицински данни (при необходимост - алергии, лекарства)

• Съгласие от ВСЕКИ родител.

ОТГОВОРНОСТИ: • Отговорник - учителят/треньорът/водачът на групата

•Хотелът обработва данни на основание договор с организатора

• Специално внимание за сигурност

X. ПРОЦЕДУРА ЗА ПРОСЛЕДЯВАНЕ НА НЕОБХОДИМОСТТА ОТ ОБРАБОТВАНЕ НА ДАННИТЕ И СРОКОВЕТЕ ЗА СЪХРАНЕНИЕТО ИМ. ОТГОВОРНИ ЛИЦА

В изпълнение на задълженията си като Администратор на лични данни и с оглед на практическото приложение на принципите на ОРЗД и по-конкретно принципите за законосъобразност, добросъвестност и прозрачност на обработването, ограничение на целите и на съхранението, свеждане на данните до минимум и отчетност на дейностите по обработване, събраните и съхранявани от „САЗА ТУР" ЕООД лични данни подлежат на периодична проверка относно необходимостта от тяхното по-нататъшно обработване и сроковете за съхранението им. Личните данни се съхраняват за период не по-дълъг от необходимото за целите, за които се обработват или от законоустановените срокове за това.

В края на всяко шестмесечие от текущата календарна година, служителите на „САЗА ТУР" ЕООД, на които е представен достъп до събраните лични данни, под ръководството и контрола на Координатора по защита на данните, проверяват обработваните и съхранявани от Дружеството лични данни на хартиен и електронен носител с оглед наличието на необходимост за по-нататъшното им обработване и проследяване на сроковете за съхранението им. За резултатите от проведената проверка Координаторът по защита на данните уведомява Управителя на Дружеството.

В случай, че по отношение на определени лични данни се установи, че е отпаднала необходимостта от обработването им и/или е постигната целта, за която са били събрани и/или са изтекли сроковете за съхранение, както са определени в Приложение № 1 за съответния регистър, те се унищожават съгласно предвиденото в Раздел XIV по-долу.

При изтичане на срока за съхранение на личните данни от съответния регистър, както е посочен в Приложение № 1 към настоящата Политика, личните данни се отбелязват като подлежащи на унищожаване и се унищожават.

XI. ПРЕДОСТАВЯНЕ НА ЗАДЪЛЖИТЕЛНА ИНФОРМАЦИЯ НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ. ОТГОВОРНИ ЛИЦА

11.1. Изисквания към предоставяната информация

В изпълнение на принципа за законосъобразно, добросъвестно и прозрачно по отношение на субектите обработване на лични данни, във всеки случаи на обработване на лични данни в качеството си на Администратор „САЗА ТУР" ЕООД предоставя на субектите на данни определена информация за извършваното обработване, която:

1) е в кратка, разбираема и лесно достъпна форма;

2) е изготвена на ясен и прост език;

3) разяснява:

- правното основание и целите на обработването;
- източника на лични данни (ако е различен от самия субект);
- получателите или категориите получатели на данните;
- евентуалното предоставяне на данните на трета държава;
- срока на обработването;
- правата на физическите лица.

11.2. Срокове за предоставяне на информацията

Информацията се предоставя на лицата в следните срокове:

- При получаване на личните данни от субекта на данните -в момента на получаването на данните;

- При получаване на личните данни от друг източник - в разумен срок след това, но не по-дълъг от 1 месец, освен ако първият контакт със субекта на данните или първото им предаване на друг получател не се извършва по-рано (в който случай предоставянето на информацията се извършва при първия контакт със субекта на данните/ преди предаването на друг получател).

11.3. Отговорни лица за предоставянето на информацията

Hotel Expo Sofia
149, Tsarigradsko Shosse blvd.
1784 Sofia, Bulgaria
T: +359 2 817 81 00 | reservations@hotelexposofia.com
www.hotelexposofia.com

Лицата, отговорни за предоставянето на информацията на субектите, чиито данни се обработват, са лицата с предоставен достъп до личните данни от съответния регистър, съгласно Приложение № 1.

XII. ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ И ПРОЦЕДУРА ЗА ТЯХНОТО РЕАЛИЗИРАНЕ. ОТГОВОРНИ ЛИЦА

За да се гарантира защитата на интересите на субектите на лични данни и сигурността на обработваните за тях лични данни, субектите разполагат с изрично регламентирани от ОРЗД права, на които съответстват определени задължения на Администратора, респективно на обработващите личните данни.

12.1. Права на субектите на лични данни

Субектите на данни имат следните права:

1) Право на достъп до обработваните лични данни - субектът на данни има право да получи потвърждение от Администратора дали се обработват лични данни, свързани с него, съответно - да получи достъп до данните и до определена информация, свързана с обработката, както следва:

- данните, които идентифицират Администратора и координатите за връзка с него,
- обработваните за субекта лични данни,
- целите на обработването на личните данни,
- правно основание за обработването (включително преследваните от Администратора законни интереси)
- получателите на личните данни,
- предаването на данните на трета държава или международна организация и подходящите гаранции във връзка с това предаване,
- източника на данните,
- срока за съхранение на данните,
-съществуването на автоматизирано вземани на решения (включително профилиране)
- право на жалба до КЗЛД,
- други права на субекта на данни във връзка с обработването.

Hotel Expo Sofia
149, Tsarigradsko Shosse blvd.
1784 Sofia, Bulgaria
T: +359 2 817 81 00 | reservations@hotelexposofia.com
www.hotelexposofia.com

2) Право на коригиране на личните данни -субектът на данни има право да поиска Администраторът да коригира без ненужно забавяне неточните лични данни, свързани с него, както и да ги допълни, там където са налице празноти, включително чрез предоставяне на декларация;

3) Право на изтриване (право „да бъдеш забравен") - субектът на данни има право да поиска от Администратора изтриване на свързаните с него лични данни без ненужно забавяне, в определени хипотези, както следва:

- личните данни повече не са необходими за целите, за които са били събирани и обработвани,
- субектът на данните оттегля даденото съгласие, въз основа на което се извършва обработването и не е налице друго основание за по-нататъшното им обработване,
- субектът на данните възразява срещу обработването и няма законни основания за обработването, които да имат преимущество над интересите на субекта,
- личните данни са били обработвани незаконосъобразно,
- личните данни трябва да бъдат изтрити с оглед спазване на правно задължение, произтичащо от българското право или правото на ЕС.

4) Право на ограничаване на обработването - субектът на данни може да поиска ограничаване на обработването, в определени хипотези, както следва по-долу. В тези случаи обработването може да се извършва само със съгласието на субекта на данни или за установяването, упражняването или защитата на правни претенции или за защита правата на друго физическо лице:

- точността на личните данни се оспорва от субекта на данните, когато срокът, позволява на Администратора да позволи точността им,
- обработването е неправомерно, но субектът не желае данните да бъдат изтрити, а изисква вместо това ограничаване на използването им,
- Администраторът не се нуждае повече от личните данни за целите на обработването, но субектът на данните ги изисква с оглед установяване, упражняване или защита на правни претенции,

Hotel Expo Sofia
149, Tsarigradsko Shosse blvd.
1784 Sofia, Bulgaria
T: +359 2 817 81 00 | reservations@hotelexposofia.com
www.hotelexposofia.com

- субектът на данните е възразил срещу обработването им - когато се очаква проверка за наличие на законни основания на Администратора, които имат преимущество пред интересите на субекта на данните.

5) Право на преносимост на данните - субектът на данни има право да получи личните данни, които го засягат и които той е предоставил на Администратора, в структуриран, широко използван и пригоден за машинно четене формат, като има право да прехвърли тези данни на друг Администратор.

Тези права лицата имат, когато:

- обработването е основано на съгласие или на договорно задължение,
- обработването се извършва по автоматизиран начин;

6) Право на уведомяване за нарушение на сигурността на личните данни- субектът на данни има право да бъде уведомен за осъществено нарушение на сигурността на личните му данни, когато има вероятност това нарушение да породи висок риск за правата и свободите на засегнатия субект на данните;

7) Право на възражение - субектът на данни има право по всяко време да възрази срещу обработването на данни, отнасящи се до него, когато обработването се извършва с оглед защита на легитимните интереси на Администратора или трета страна;

8) Право на оттегляне на съгласието за обработване - субектът на данни има право да оттегли даденото изрично съгласие за обработване по всяко време, като това не засяга законосъобразността на извършеното до този момент обработване въз основа на предварително даденото съгласие;

9) Право на жалба до надзорен орган -субектът има правото да подаде жалба до надзорен орган срещу Администратора и/или обработващ лични данни във връзка с извършваното обработване на личните му данни;

10) Право на защита по съдебен ред -субектът на данните има право да предприеме необходимите действия за осъществяване на съдебната си защита по реда, предвиден за такава защита в Регламента и/ или действащото законодателство, срещу отнасящо се до него задължително решение на надзорен орган, както и срещу действия на

Администратор и/ или обработващ лични данни по обработване на негови лични данни, с които правата му по Регламента са били нарушени.

12.2. Процедура за упражняване на правата

Правата по-горе се упражняват от субекта на данните посредством подаването на писмено искане до „САЗА ТУР" ЕООД на следния адрес: гр. Пловдив, р-н Северен, ул. Белград № 6, ет.6- на вниманието на управителя Анастасия Иванова Накова. Искането може да бъде подадено и посредством електронни средства, като за целта се изпраща до следния адрес за електронна кореспонденция:office@radis-group.com. Когато искането е подадено по електронен път, информацията във връзка с него се предоставя също посредством електронни средства, освен ако субектът на данните изрично не е поискал друго.

Информация за предприетите действия във връзка с отправеното искане се предоставя на субекта на данни в писмен вид (вкл. чрез електронно съобщение), без ненужно забавяне и най-късно в срок до 1 (един) месец от получаването му от Дружеството.

Вземайки под внимание, сложността и броя на отправените искания, „САЗА ТУР" ЕООД може да удължи срока за предоставяне на информация относно предприетите действия най-много до 2 (два) допълнителни месеца. За всяко такова удължаване „САЗА ТУР" ЕООД информира субекта на данните в срок до 1 (един) месец от получаването на първоначалното искане, като посочва и причините, наложили забавянето.

След преценка на искането с оглед на необходимите действия за удовлетворяването му и евентуалната невъзможност за тяхното извършване и/ или прекомерност на изискваните усилия за това, Дружеството може да не предприеме действия във връзка с искането на субекта на данни. В този случай, „САЗА ТУР" ЕООД уведомява субекта на данните за това без излишно забавяне и най-късно в срок от 1 (един) месец от получаване на искането като посочва и причините, поради които няма да предприеме действия за удовлетворяването му. В тази връзка, субектът на данните се уведомява и за възможността си да подаде жалба до надзорен орган и/или да потърси защита по съдебен ред, в съответствие с правата по-горе.

12.3. Ред за упражняване на правата по т. 12.1, т.9

Надзорният орган, който е компетентен да разглежда подадените жалби във връзка с обработваните лични данни на територията на Република България е Комисията за защита на личните данни (КЗЛД).

Жалби към КЗЛД във връзка с незаконосъобразно и/или неправомерно обработване на лични данни, могат да бъдат подавани лично, по пощата и/или чрез куриер или посредством електронна поща, както следва:

Адрес: гр. София 1592, бул. Проф. Цветан Лазаров № 2,

Електронна поща: kzld@cpdp.bg,

Интернет страница: www.cpdp.bg

12.4. Отговорни лица за изпълнението на процедурата

След получаване на искането от субекта на личните данни, Координаторът по защита на данните, заедно с лицата, на които е възложено обработването на личните данни на субекта, изготвят проект на отговор, който се съгласува с Управителя на Дружеството.

XIII. ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ ИНЦИДЕНТИ. ПРОЦЕДУРА ЗА ДОКЛАДВАНЕ И УПРАВЛЕНИЕ НА ИНЦИДЕНТИ. РЕАКЦИЯ ПРИ НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

13.1. Процедура за докладване и управление на инциденти

При възникване на инцидент (произшествие, авария, бедствие или друго непредвидимо обстоятелство, което може да засегне сигурността на личните данни), лицата, на които е възложено обработването на данните са длъжни да информират незабавно Управителя на Дружеството, както и да вземат необходимите мерки за предотвратяване или ограничаване увреждането на регистрите на лични данни. Тези действия се извършват при спазване на всички останали изисквания за безопасност и без риск за здравето и живота на членовете на персонала на Дружеството.

В случай, че се касае за кражба или друго неправомерно отнемане на имущество или информация, незабавно се уведомяват органите на полицията, застрахователят, охранителното дружество, както и други компетентни лица, ако това се изисква от действащото законодателство с оглед на обстоятелствата.

За всеки инцидент, довел до увреждане на съхранявани лични данни, се съставя протокол от Координатора по защита на данните и/или от лицата, пряко обработващи засегнатите данни, който съдържа: времето на възникване на инцидента и времето на неговото установяване, причините за инцидента, нанесените вреди и предприетите мерки за ограничаването им, както и препоръки за предотвратяване на повторен инцидент.

В случай, че за възникване на инцидента бъде установена вина на служители на Дружеството, се предприемат действия по търсене на съответна дисциплинарна и/ или гражданска отговорност съгласно изискванията на действащото законодателство.

13.2. Реакция при нарушение на сигурността на личните данни

В случай на установено нарушение на сигурността на личните данни по смисъла на настоящата Политика и Регламента, Дружеството документира в писмен вид всяко нарушение на сигурността на личните данни, посочвайки фактите, свързани с него, настъпилите последици и предприетите мерки и действия за отстраняване на нарушението и последиците от него.

Дружеството в качеството си на Администратор на личните данни, по отношение на които е осъществено нарушението на сигурността, уведомява без ненужно забавяне КЗЛД, в качеството му на надзорен орган, но не по-късно от 72 (седемдесет и два) часа от момента на узнаване на нарушението, когато това е възможно. Когато не е възможно информацията да се подаде едновременно, тя се подава поетапно, без ненужно забавяне.

Уведомлението за нарушение на сигурността на личните данни до КЗЛД следва да съдържа най-малко следната информация:

1) Описание на естеството на нарушението, а по възможност и категориите и приблизителното количество/ броя засегнати записи на лични данни и субекти на лични данни;

2) Информация за контакт с отговорното лице от Дружеството, подало уведомлението;

3) Описание на последиците, които са възникнали или биха могли да възникнат вследствие на осъщественото нарушение;

4) Информация за предприетите и/или приложени мерки от Дружеството за справяне с нарушението на сигурността на личните данни и намаляване на евентуално настъпилите неблагоприятните последици от него;

5) Причините за забавяне при подаване на уведомлението, ако то е подадено след срока от 72-часа.

Когато е налице вероятност нарушението на сигурността на личните данни да породи висок риск по отношение на правата и свободите на засегнатите субекти на данни, Дружеството съобщава на субекта на данните в писмен вид и без ненужно забавяне за осъщественото нарушение и настъпилите последици от него.

Това съобщение се изготвя на ясен и разбираем за субекта на данните език и включва информацията по т. 1) до 6) включително, по-горе.

Такова информиране на субекта може да не се извършва, когато:

1) Дружеството е предприело подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността (по-конкретно мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране);

или

2) Дружеството е взело впоследствие мерки, които гарантират, че вече няма опасност за правата и свободите на субектите на данни; или

3) Индивидуалното информиране на всеки субект на данни би довело до непропорционални усилия. В такъв случай Дружеството извършва публично съобщение или предприема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

XIV. УНИЩОЖАВАНЕ НА ЛИЧНИТЕ ДАННИ СЛЕД ПОСТИГАНЕ НА ЦЕЛИТЕ НА ОБРАБОТВАНЕТО

След като целта на обработването на личните данни бъде постигната и/или след изтичане на определените в Приложение № 1 срокове за съхранение на данните,

„САЗА ТУР" ЕООД унищожава съответните лични данни като взема адекватни мерки с цел да не се допусне неоторизиран достъп до личните данни по време на унищожаването им.

Определянето на личните данни, които следва да бъдат унищожени, се извършва въз основа на проведена проверка за проследяване на необходимостта от обработване на данните и сроковете за съхранението им.

Унищожават се само документите на хартиен и/или електронен носител, съдържащи лични данни, които не подлежат на връщане на субектите на лични данни, или на предаване на компетентен публичен орган в изпълнение на законоустановено задължение на „САЗА ТУР" ЕООД в качеството му Администратор на лични данни (например Националния осигурителен институт).

14.1. Унищожаване на данни на хартиен носител

Унищожаването на личните данни от различните регистри, поддържани от „САЗА ТУР" ЕООД, които се съхраняват и обработват на хартиен носител, се извършва от съответните служители и/или определените лица, на които е възложено обработването на личните данни и им е предоставен достъп до тях, съгласно Приложение № 1 към настоящата Политика.

Подлежащите на унищожение документи се предават на Координатора по защита на данните след завършване на годишното архивиране и съставяне на списък с файловете, подлежащи на унищожаване. Документите се унищожават посредством шредер за хартия.

14.2. Унищожаване на данни на електронен носител

Унищожаването на личните данни от различните регистри, поддържани от „САЗА ТУР" ЕООД, които се съхраняват и обработват на електронен носител, се инициира от съответните служители и/или определените лица, на които е възложено обработването на личните данни и им е предоставен достъп до тях, съгласно Приложение № 1 към настоящата Политика.

Личните данни, съхранявани на персоналните компютри, в т.ч. и личните данни, съхранявани в електронната поща под формата на имейли и/или прикачени файлове, се преглеждат и се унищожават от съответния служител, ползващ устройството.

Всички лични данни, съхранявани и обработвани на преносим електронен носител (CD/ DVD/ BRD/ USB Memory Stick) и/или на твърд диск на преносим или стационарен компютър се унищожават от съответния служител под наблюдението и със знанието на прекия му ръководител, като се използват подходящи за това програми.

XV.ОТСЪСТВИЕ НА ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ (DPO)

15.1. Оценка на необходимостта

„САЗА ТУР" ЕООД е извършило оценка на дейността си и е установило, че назначаването на Длъжностно лице по защита на данните (Data Protection Officer - DPO) не е задължително на основание чл. 37 от Регламента, тъй като:

1) Дружеството не е орган или публична институция;

2) Основната дейност на Дружеството не се състои в операции по обработване, които поради своя характер, обхват и/или цели изискват редовно и систематично мониторинг на субектите на данни в широкомащабен мащаб;

3) Основната дейност на Дружеството не се състои в широкомащабно обработване на специални категории данни по чл. 9 от Регламента.

15.2. Функции на отговорните лица

Въпреки че не е назначено DPO, функциите по защита на данните се изпълняват от определени отговорни лица:

1) Управителят на Дружеството е отговорен за:

- Общото спазване на изискванията на Регламента;
- Одобрение на политики и процедури за защита на данните;
- Вземане на решения относно обработването на лични данни;
- Комуникация с Комисията за защита на личните данни при необходимост;

2) Определен служител (Координатор по защита на данните) е отговорен за:

- Консултиране относно задълженията за защита на данните;
- Наблюдение на спазването на политиките;
- Обучение на персонала;
- Взаимодействие със субектите на данни;

- Поддържане на регистъра на дейностите по обработване.

15.3. Контакти за въпроси относно защита на данните

За всички въпроси, свързани със защитата на личните данни, субектите могат да се свържат с:

Наименование: „САЗА ТУР" ЕООД

Адрес: гр. Пловдив, ул. Белград № 6, ет.6

Телефон: 0878051281

Имейл: office@radis-group.com

Управител: Анастасия Накова

XVI. АКТУАЛИЗАЦИЯ И ПРЕГЛЕД НА ПОЛИТИКАТА

Настоящата Политика подлежи на редовен преглед и актуализация:

1) Минимум веднъж годишно от Управителя на Дружеството;

2) При всяка съществена промяна в дейността на Дружеството;

3) При промени в приложимото законодателство;

4) При внедряване на нови технологии или процеси на обработване;

5) При препоръки от Комисията за защита на личните данни.

Всички промени в Политиката се одобряват със Заповед на Управителя и се довеждат до знанието на персонала.

„САЗА ТУР" ЕООД, в качеството си на Администратор на лични данни, си запазва правото да изменя и обновява настоящата Политика за защита на личните данни и Приложенията към нея по всяко време с оглед на евентуални промени в режима на защитата на личните данни и приложимото европейско и национално законодателство в тази област, както и при настъпили промени в извършваната обработка и/ или прилаганите практики и процедури в тази връзка.

Настоящата Политика е утвърдена със Заповед на Управителя на „САЗА ТУР" ЕООД и влиза в сила от деня на утвърждаването ѝ.

Настоящата Политика и правилата, установени в нея се прилагат по отношение на всички лични данни, обработвани от Дружеството в качеството му на Администратор съгласно Приложения № 1 и спазването ѝ е задължително за

персонала на Дружеството (вкл. изпълнители по граждански договори, стажанти и командировани служители) и членовете на неговите органи на управление.