**Одобрил:**

Любомир Хайнов / Lubomir Hainov

Изпълнителен директор – Челопеч / General manager – Chelopech

ДПМ Челопеч ЕАД / Dundee Preacious Metals Chelopech EAD

**Дата:**_____

**Approved by:**

Ирена Цакова/Irena Tsakova

Изпълнителен директор – Ада Тепе / General manager – Ada Tepe

ДПМ Крумовград ЕАД / Dundee Preacious Metals Krumovgrad EAD

**Date:**

| | |
|---|---|
| *Privacy standard* | *Стандарт за неприкосновеност на личните данни* |
| Document Number: GRP-ST-LEG-19 V.1.1 | Код на документа: GRP-ST-LEG-19 V.1.1 |
| Policy Document Owner_____ | Собственик: _____ |
| Policy Document Approver _____ | Утвърдил: _____ |

# Document Administration

## Document Management

| | |
|---|---|
| **Document Owner (Name, Title)** | Kelly Stark-Anderson, Executive Vice President, Corporate Affairs, General Counsel and Corporate Secretary |
| **Document Administrator (Name, Title)** | Petya Dombalova, Director Legal & Compliance |
| **Document Approver (Group or Name, Title)** | David Rae, President and Chief Executive Officer |
| **Adoption Date** | May 1, 2025 |
| **Initial Effective Date** | June 1, 2025 |
| **Last Amended Date** | September 12, 2025 |
| **Effective Date of the Last Amendment** | September 12, 2025 |
| **Next Review Date** | May 1, 2027 |

## Version History

| Version | Description of Version Changes |
|---|---|
| 1.0 | Initial |
| 1.1 | Revised (2025: company name and logo changes) |

## Related Policy Documents

| Document Number | Document Title |
|---|---|
| *GRP-PO-LEG-01 V.10* | *Code of Business Conduct and Ethics* |
| *GRP-PO-IT-01 V.3.1* | *Information Protection Policy* |
| *GRP-ST-IT-06 V.2.0* | *Information Categorization Standard* |
| *GRP-ST-IT-05 V.1.0* | *Data Loss Prevention Standard (under Revision)* |

# Администриране на документа

## Управление на документа

| | |
|---|---|
| **Собственик на документа (име и длъжност)** | Кели Старк-Андерсън, Изпълнителен вицепрезидент “Корпоративни отношения”, Главен юрисконсулт и Корпоративен секретар |
| **Администратор на документа (име и длъжност)** | Петя Домбалова, директор правни въпроси и съответствие |
| **Утвърдил (групов орган или име и длъжност)** | Дейвид Рей, президент и главен изпълнителен директор |
| **Приет на** | 1 май, 2025 |
| **В сила от** | 1 юни, 2025 |
| **Дата на последно изменение** | 12 септември 2025 |
| **Дата на влизане в сила на последното изменение** | 12 септември 2025 |
| **Дата на следващ преглед** | 1 май, 2027 |

## Предишни версии

| Версия | Описание на промените във версиите |
|---|---|
| 1.0 | Първоначална версия |
| 1.1 | Редакция (2025: ново име и лого на компанията) |

## Свързани политики

| Код на документа | Наименование |
|---|---|
| *GRP-PO-LEG-01 V.10* | *Правилник за бизнес поведение и етика* |
| *GRP-PO-IT-01 V.3.1* | *Политика за защита на информацията* |
| *GRP-ST-IT-06 V.2.0* | *Стандарт за категоризиране на информацията* |
| *GRP-ST-IT-05 V.1.0* | *Стандарт за предотвратяване на загубата на данни* |

| | |
|---|---|
| *GRP-ST-IT-04 V.2.0* | *Information Retention, Recovery and Sanitization Standard* |
| *GRP-ST-LEG-17 V.1.1* | *Subsidiary Governance Standard* |
| *GRP-PR-IT-12 V.2.0* | *Acceptable Mobile Device Use Procedure* |
| *GRP-PR-IT-09 V.2.1* | *Acceptable Email Use Procedure* |
| *GRP-PR-IT-11 V.2.0* | *Internet Acceptable Use Procedure* |

| | |
|---|---|
| *GRP-ST-IT-04 V.2.0* | *Стандарт за съхранение, санитизиране и възстановяване на данни* |
| *GRP-ST-LEG-17 V.1.1* | *Стандарт за управление на дъщерните дружества* |
| *GRP-PR-IT-12 V.2.0* | *Процедура за защита и допустима употреба на мобилните устройства* |
| *GRP-PR-IT-09 V.2.1* | *Процедура за допустимо използване на електронна поща* |
| *GRP-PR-IT-11 V.2.0* | *Процедура за допустимо използване на Интернет* |

## Table of Contents



## Съдържание

## 1 Defined Terms

## 1 Дефиниции на термини

The following terms and acronyms are integral to the understanding of this Standard and have the meanings assigned within this Section or as referenced herein:

Термините и съкращенията по-долу са важни за правилното разбиране на настоящия стандарт и са използвани със следните значения:

| Term | Definition | Термин | Дефиниция |
|---|---|---|---|
| Board Member(s) | As a group or individually, any member of the DPM Board or any member of the board of directors of any DPM subsidiary or any individual delegated equivalent authority by the shareholder(s) of such entity. | Членове на Борда | Заедно или поотделно – всяко лице в състава на Борда на директорите на ДПМ или на някое от дъщерните ѝ дружества, както и всяко лице, на което акционер(и) на тези дружества са възложили еквивалентни правомощия. |
| Business Function and Business Function Head | A team of Employees with a designated cost centre, or multiple cost centres, accountable for establishing and maintaining business systems, including through Policy Documents, internal controls, and applications; managing or supporting implementation; and providing ongoing support to other Employees and relevant Third Parties. The Business Function Head thereof is the individual accountable for the Business Function. | Бизнес функция и ръководител на бизнес функция | Екип от работници/служители с отделен разходен център или с няколко разходни центрове, чиито отговорности включват изграждане и поддържане на бизнес системи, включително чрез фирмени политики, вътрешни мерки за контрол и различни приложения; управление и съдействие за внедряване; оказване на подкрепа на други работници/служители и трети страни. Отговорността за Бизнес функцията се носи от нейният ръководител. |
| Business Unit and Business Unit Head | DPM and each of its Subsidiaries, individually. The Business Unit Head is the individual accountable for the Business Unit. | Бизнес единица и ръководител на бизнес единица | ДПМ и всяко от дъщерните ѝ дружества поотделно. Ръководителят е лицето, което носи отговорност за бизнес единицата. |
| Collect, Collected or Collection | The gathering, acquiring or otherwise obtaining, recording, and / or compiling of Personal Information. | Събиране, събрана, сбор от информация | Събиране, придобиване или по друг начин получаване, записване и/или компилиране на Лични данни. |
| Company or Group | DPM and all its directly and indirectly owned Subsidiaries, collectively. | Компания или Група | ДПМ и всички дъщерни дружества, чиито капитал компанията притежава пряко и непряко, взети заедно. |
| Consent | An agreement to the Collection, Use, and / or Disclosure of Personal Information. | Съгласие | Съгласие за събиране, използване или разкриване на Лични данни. |
| Corporate Compliance Officer | The Corporate Director Legal & Compliance or any other Employee appointed as Corporate Compliance Officer by the DPM Board. | Корпоративен отговорник по съответствието | Корпоративният директор „Правни въпроси и съответствие” или друг служител, назначен от Борда на ДПМ на длъжност корпоративен отговорник по съответствието. |
| Data Processing Agreement or DPA | A legally binding document that outlines the terms and conditions under which Personal Information is Processed by a Third-Party Processor on behalf of the Company including but not limited to the rights and obligations of both the Third-Party Processor and the Company. | Споразумение за обработка на Лични данни | Правно обвързващо споразумение, което определя изискванията и условията за обработване на лични данни от Трета страна от името на Компанията, включително, но не само, правата и задълженията на обработващата Трета страна и на Компанията. |

| | | | |
|---|---|---|---|
| Disclose, Disclosed or Disclosure | The transmission, dissemination, or otherwise making available of Personal Information. | Разкрива, разкрита и разкриване | Предаване, разпространение или по друг начин предоставяне на Лични данни |
| DPM | DPM Metals Inc. (the parent company incorporated in Canada). | ДПМ | „ДПМ Металс“ Инк. (компанията-майка, учредена в Канада) |
| Employee | An individual engaged by the Company on a full-time or part-time permanent, fixed term, or temporary basis, as well as a secondment employee, student, intern, or apprentice. For clarity, Employees also include Company Officers. For the definition of “Company Officer”, refer to the *Subsidiary Governance Standard.* | Работник/служител | Лице, нает от компанията по трудово правоотношение на пълно или непълно работно време със срочен или безсрочен договор, включително и командировано на друго работно място или временно нает студент, стажант или практикант. За повече яснота категорията „работник/служител“ включва и членовете на висшето ръководство на компанията. За целите на дефиницията “Длъжностно лице на Компанията”, прави препратка към *Стандарта за управление на дъщерните дружества.* |
| Group Privacy Officer | The Corporate Compliance Officer or any other person designated by DPM’s Chief Executive Officer. | Отговорник за Лични данни в Групата ДПМ | Корпоративният отговорник по съответствието или друго лице, определено от Главния изпълнителен директор на ДПМ. |
| Information Subject | The identified or identifiable living individual to whom Personal Information relates. | Субект на Лични данни | Идентифицирано или възможно за идентифициране живо физическо лице, за което се отнасят определени Лични данни |
| IT Privacy Coordinator | A member of the Company’s Technology Function, designated by the VP Supply Chain & Technology, to carry out the Privacy-related accountabilities set out in this Standard. | ИТ Координатор за Лични данни | Член на ИТ екипа на компанията, определен от Вицепрезидент “Верига на доставките и Технологии” за изпълнение на отговорностите по защита на Личните данни съгласно настоящия Стандарт. |
| Personal Information | Any information that identifies an Information Subject, or information relating to an Information Subject, that the Company can directly or indirectly identify from the information alone or combined with other identifiers that the Company possesses or can reasonably access. This includes identifiers such as name, identification number, location data, online identifier, factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that Information Subject. | Лични данни/ Лична информация | Всяка информация, която идентифицира Субекта на данните/информацията, или и информация, свързана с този Субект, която Компанията може да идентифицира директно или, индиректно от самите данни или комбинация с други идентификатори, които Компанията притежава или до които може да има достъп. Това включва идентификатори като име, идентификационен номер, данни за местоположение, онлайн идентификатор, фактори, които конкретно се отнасят за физическата, физиологичната, генетична, психическа, икономическа, културна и социална идентичност на Субекта на данните/информацията. |

| | | | |
|---|---|---|---|
| Personal Information Breach | Any act or omission that compromises the security, confidentiality, integrity or availability of Personal Information or the physical, technical, administrative or organizational safeguards that the Company or its Third-Party Processor put in place to protect it. The loss, or unauthorized access, disclosure or acquisition, of Personal Information is a Personal Information Breach. | Нарушение на сигурността на Личните данни | Всяко действие като пропуск или компрометиране на сигурността, конфиденциалността, интегритета или наличието на Лични данни или физическите, технически, административни и организационни защити на данни, въведени в Компанията или Трета страна, която обработва данни. Загубата или неоторизираният достъп, разкриване или придобиване на Лични данни/информация представлява неоторизирано разкриване на Лични данни. |
| Policy Document | Each or any of a Policy, Standard, Procedure or Guideline created by or for the Company or one or more of its Business Units. | Политика на Компанията | Политика, стандарт, процедура, насоки, разработени от или за компанията или нейна бизнес единица. |
| Privacy | The protection of Personal Information Processed by or on behalf of the Company. | Неприкосновеност на информацията | Представлява защита на Личните данни/ информация, която се обработва от или от името на Компанията. |
| Privacy Laws | All laws and regulations pertaining to Personal Information protection, that are applicable to the Company, including but not limited to the *Canadian Personal Information Protection and Electronic Documents Act* (PIPEDA) and the European Union *General Data Protection Regulation* (GDPR). | Закони за Личните данни | Всички закони и наредби, касаещи защита на Личните данни, които следва да се спазват от компанията, в това число но не единствено, канадския *Закон за защита на личните данни и електронните документи* и *Общия регламент за защита на личните данни* (GDPR) на ЕС. |
| Privacy Liaison | The Head of, or an Employee designated by the Head of, the Business Function Collecting or otherwise Processing Personal Information to carry out the Privacy - related accountabilities set out in this Standard. | Лице за контакт по отношение на Личните данни | Ръководител на или служител за защита на неприкосновеността на Личните данни, определен от Ръководителя на бизнес функцията, която събира или по друг начин обработва Лични данни - свързаните са това отговорности са определени в настоящия Стандарт. |
| Privacy Professionals | A member of the Legal & Compliance Function at each respective Business Unit, who has been assigned Privacy accountabilities for the Business Unit by the Business Unit Head. | Специалисти по неприкосновеност на Личните данни | Член на функцията “Правни въпроси и съответствие” във всяка от бизнес единиците, на когото Ръководителят на бизнес единицата е възложил отговорности за неприкосновеността на Личните данни в бизнес единицата. |

| | | | |
|---|---|---|---|
| Process, Processed or Processing | In the context of Personal Information, the verb “to process” includes any activity that involves the use of Personal Information (whether through manual or automated means) such as the Collection, recording, storage, retrieval, use (i.e., organization, adaption, alteration, consultation, alignment, or combination), Disclosure and destruction of Personal Information. Processing also includes transmitting or transferring Personal Data to Third Parties. | Обработване, обработени или процес на обработка | В контекста на Личните данни /информация, глаголът „обработвам” включва всяка дейност с Лична информация чрез ръчни или автоматизирани дейности, свързани със събиране, съхранение, извличане, използване (т.е. организиране, адаптиране, изменение, консултиране, хармонизиране или комбинация), разкриване (т.е. организиране, адаптиране, изменение, консултиране, синхронизиране и комбиниране), разкриване и унищожаване на лични данни/ информация. Обработката включва и предаване или прехвърляне на Лични данни към Трети страни. |
| Subsidiary | Includes each entity in which DPM holds, directly or indirectly, over 50% ownership of the voting shares or an interest which allows DPM to exert direct or indirect control over the entity (collectively referred to as Subsidiaries). For clarity, the Private English Language Secondary School Chelopech EOOD is not included in this definition as it is subject to the *Bulgarian Education Act*. | Дъщерно дружество | Включва всяко юридическо лице, в което ДПМ държи директно или индиректно 50% от акциите с право на глас или интерес, който позволява на ДПМ да упражнява директен или индиректен контрол върху юридическото лице (заедно наричани “Дъщерните дружества”). За повече яснота „Частната профилирана гимназия с чуждоезиково обучение „Челопеч“ ЕООД се изключва от тази категория, тъй като се подчинява на *Закона за образованието*. |
| Third Party | An individual, company, or other entity, that is interested in entering or has an existing business relationship with the Company. Third Parties include, but are not limited to, suppliers, contractors, advisors, consultants, agents, brokers, lobbyists, donation and sponsorship beneficiaries, customers, and joint venture, merger, and acquisition partners. | Трета страна | Физическо лице, дружество или друго юридическо лице, което е в бизнес отношения или има интерес да установи такива отношения с Компанията. Категорията включва, но не се ограничава до доставчици, външни изпълнители, съветници, консултанти, агенти, брокери, лобисти, бенефициенти на дарения и спонсорство, клиенти и партньори в съвместни предприятия, сливания и придобивания. |
| Third-Party Processor | Third-Party Processors are Third Parties engaged by the Company to Process the Personal Information as further set out in Section 4.7. | Трета страна, която обработва Лични данни | Обработваща трета страна представлява Трета страна, която Компанията е ангажирала да обработва Лични данни съгласно текста на Раздел 4.7. |

| 2 Purpose and Scope | 2 Цел и обхват |
|---|---|
| | |
| The purpose of this Privacy Standard (this Standard) is to facilitate the protection of Personal Information the Company Collects and otherwise Processes (including the Personal Information of Employees, Board Members, and Third-Party Information Subjects) in accordance with applicable legal requirements. | Целта на настоящия Стандарт за неприкосновеност на личните данни е да подпомогне защитата на Личните данни, които Компанията събира или по друг начин обработва (включително Лични данни на работници/служители, членове на Борда, и Трети страни които са Субект на данни). |
| | |
| This Standard sets out the Company's approach to using, managing and protecting Personal Information, regardless of the medium on which that information is stored, and is applicable to Board Members, Employees and Third Parties, who Process Personal Information at the request and/or on behalf the Company. | Настоящият Стандарт определя подхода на Компанията по отношение на използването, управлението и защитата на Личните данни, независимо от средата, в която се съхраняват. Този Стандарт е приложим за членовете на Борда, работници/служители и Трети страни, които обработват Лични данни по искане или от името на Компанията. |
| | |
| **3 Overarching Requirements** | **3 Общовалидни изисквания** |
| | |
| The Company operates across different jurisdictions, each with its own set of Privacy Law requirements. It is committed to complying with all applicable Privacy Laws and adhering to the principles outlined in the Information Protection Policy. This Standard establishes the requirements that will be uniformly applied across all jurisdictions where the Company conducts business. In instances where local Privacy Laws impose additional or more stringent standards, those higher requirements must be observed. | Компанията работи в различни юрисдикции, всяка от които има собствени нормативни изисквания за неприкосновеността на Личните данни. Компанията е поела ангажимент да спазва всички приложими нормативни изисквания и принципите, заложени в Политиката за защита на информацията. Настоящият Стандарт определя единни изисквания, които ще се прилагат във всички юрисдикции, в които Компанията работи. В случаите, когато местните закони за неприкосновеност на Личните данни определят по-стриктни стандарти, Компанията трябва да спазва тях. |
| | |
| A fundamental principle of this Standard is the recognition that Personal Information is owned by the Information Subject, not by the Company. Consequently, the Company is dedicated to respecting and safeguarding the Personal Information of Employees and Third Parties, which it Processes. This commitment is paramount to maintaining the trust and confidence of all Company's stakeholders. A failure to protect Personal Information can also result in legal and reputational risk to the Company. | Фундаментален принцип на настоящия Стандарт е презумпцията, че Субектът на данни е собственикът на Личните данни а не Компанията. В този смисъл, Компанията е поела ангажимент да уважава и пази Личните данни на работниците/служителите и на Трети страни, която обработва. Този ангажимент е основополагащ за поддържането на доверието и сигурността на всички заинтересовани страни на Компанията. Неуспешната защита на Личните данни може да представлява правен и репутационен риск за Компанията. |
| | |
| This Standard must be read in conjunction with the Policy Documents listed in the Related Documents Section. | Настоящият Стандарт трябва да се тълкува и прилага съвместно с документацията, посочена в раздел "Свързани документи". |
| | |

| 4 Performance Requirements | 4 Изисквания за изпълнение |
|---|---|
| | |
| 4.1 Permissibility of Personal Information Processing | 4.1 Допустимост на обработката на Лични данни. |
| | |
| The Processing of Personal Information is allowed only if the Information Subject has given their Consent or if it is otherwise permitted by applicable Privacy Laws. | Обработката на Лични данни е позволена само, ако Субектът на данни е дал Съгласие за това или обработката е била разрешена от приложимите регулации за неприкосновеност на Личните данни. |
| | |
| When relying on Consent for Processing, such Consent must be obtained in writing or through other legally permissible means. Prior to seeking Consent, the Information Subject must be informed about the purpose of the Processing and any potential transfer of their Personal Information. The declaration of Consent must be clearly highlighted when included within other statements to ensure it is fully understood by the Information Subject. | При позоваване на такова Съгласие, то трябва да бъде дадено в писмена форма или по друг начин, уреден от закона. Преди да се иска съгласие от него, Субектът на данни трябва да бъде информиран за целите на обработката и за потенциално прехвърляне на Личните данни. Текстът, с който се заявява Съгласие трябва да бъде подчертан и ясен, дори ако е част от по-голям текст, за да е сигурно, че е добре разбран от Субекта на данни. |
| | |
| Privacy Liaisons must keep records of all Consents related to their respective Business Functions. This ensures that the Information Subject can, if they choose, withdraw their Consent in accordance with applicable Privacy Laws. | Лицето за контакти по отношение на Личните данни трябва да поддържа записи на всички декларации за Съгласие, свързани със съответната Бизнес функция. Така се гарантира, че когато реши, Субектът на данни може да оттегли Съгласието си съгласно приложимото законодателство за Неприкосновеност на личните данни. |
| | |
| 4.2 Sensitive Personal Information and other Special Categories | 4.2 Чувствителни Лични данни и Специални категории |
| | |
| Information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, or data concerning health, sex life or sexual orientation is considered sensitive Personal Information. Other types of Personal Information may also be deemed sensitive based on the context, volume and intended usage, as determined through a Privacy Impact Assessment (see Section 4.11 below). | Информацията, която разкрива расов или етнически произход, политически мнения, религиозни или философски вярвания, членство в профсъюзи, генетични данни, биометрични данни, или данни свързани със сексуалния живот и ориентация се считат за чувствителни Лични данни. Има и други Лични данни, които може да се считат за чувствителни за конкретен контекст, обем и ползване, определени с Оценка на въздействието върху неприкосновеността на данните (виж Раздел 4.11 долу). |
| | |
| Sensitive Personal Information is subject to heightened security measures and can only be Processed with explicit consent except where required or permitted by law, such as for regulatory compliance, legal proceedings, or the protection of rights and safety. | Чувствителните Лични данни подлежат на по-строги мерки за сигурност и може да се обработват само с изрично съгласие, освен ако обработката се изисква или е разрешена по нормативен ред, т.е. съгласно нормативни изисквания, съдебно производство или действия за защита на права и сигурност. |
| | |

| | |
|---|---|
| To ensure that sensitive Personal Information is properly Processed, Privacy Liaisons must always consult with Privacy Professionals before collecting such Personal Information. Additionally, Privacy Professionals must be consulted whenever there is uncertainty whether the Personal Information to be Processed qualifies as sensitive. | За да се осигури правилната обработка на Чувствителни лични данни, Лицата за контакт по отношение на Личните данни трябва задължително да се консултират със Специалисти по неприкосновеността на Личните данни още преди да събират такива данни. Освен това, консултации със Специалистите по неприкосновеност на Личните данни трябва да се провеждат когато няма яснота дали ще се обработват Лични данни, които са категоризирани като чувствителни. |
| | |
| ## 4.3 Purpose Limitation | ## 4.3 Ограничения на целите |
| Personal Information must be Collected solely for specified, explicit and legitimate purposes. Privacy Liaisons, in consultation with the respective Privacy Professional, must define these purposes and ensure they are appropriately documented. Processing Personal Information for purposes other than those for which it was initially Collected is permissible only with the Information Subject's Consent or if otherwise allowed by applicable Privacy Laws. | Личните данни се събират само за изрично заявените и законни цели. Лицата за контакт по отношение на Личните данни са длъжни да определят тези цели и да следят за тяхното документиране. Обработката на Лични данни за други цели извън целите, за които е събрана първоначално, е разрешена само ако е събрана със Съгласието на Субекта на Лични данни или това по друг начин е разрешено от законодателството за неприкосновеността на Личните данни. |
| | |
| ## 4.4 Accuracy | ## 4.4 Точност |
| | |
| To ensure the integrity of Personal Information and protect the rights of Information Subjects, the Personal Information Processed by the Company must be accurate and up to date. The accuracy of any Personal Information Collected by the Company must be verified at the point of Collection and at regular intervals thereafter. Privacy Liaisons must also ensure that reasonable steps are taken to amend or destroy any inaccurate or outdated Personal Information Processed by their Business Function in accordance with the *Information Retention, Recovery and Sanitization Standard*. | За да се осигури интегритетът на Личните данни и да се защитят правата на Субекта на данни, информацията, която Компанията обработва, трябва да бъде точна и актуална. Точността на Личните данни, събрани от Компанията, трябва да бъде потвърдена в точката, в която се събират и след това да се потвърждава редовно. Лицата за контакт по отношение на Личните данни трябва да осигурят предприемане на разумни стъпки за редактиране или унищожаване на неточни или остарели Лични данни, които се обработват от Бизнес функция съгласно *Стандарта за съхранение, санитизиране и възстановяване на данни.* |
| | |
| ## 4.5 Reduced Data Retention | ## 4.5 Съкращаване на срока на съхранение на данни |
| | |
| The longer Personal Information is retained, the greater the risk of a Personal Information Breach or the information becoming inaccurate. The Company must ensure that Personal Information is retained only for the duration necessary to fulfill the business purpose or to comply with legal requirements. | Колкото по-дълго време се съхраняват Лични данни, толкова е по-голям рискът те да станат неточни или да бъдат разкрити чрез неоторизиран достъп. Компанията трябва да се погрижи Личните данни да се съхраняват само за срока, необходим за изпълнение на бизнес целите или за спазване на дадени правни изисквания. |
| | |

| | |
|---|---|
| Once Personal Information is no longer needed by a Business Function for its specified purposes, it must be deleted, anonymized or otherwise managed in accordance with the *Information Retention, Recovery and Sanitization Standard.* | В момента, в който Личните данни вече не са необходими на Бинес функцията за конкретни цели, те трябва да бъдат изтрити, анонимизирани или по друг начин управлявани съгласно *Стандарта за сънитизиране и възстановяване на данни* |
| | |
| ## 4.6 Personal Information Communications and Notices | ## 4.6 Лични данни, комуникация и уведомления |
| | |
| In certain jurisdictions where the Company operates, when Personal Information is Collected, Information Subjects have specific rights. Therefore, before Collecting any Personal Information, the Privacy Liaisons must consult with the respective Privacy Professional to determine what communication or formal notice, if any, must be provided to the Information Subject. | В някои юрисдикции, в които работи Компанията, Субектът на данни има конкретни права, когато се събират Лични данни. В този смисъл, преди събиране на Лични данни, Лицата за контакт по отношение на Личните данни трябва да се консултират със Специалистите по неприкосновеност, за да се установи дали на Субекта на данни трябва да се изпрати някакво съобщение или официално уведомление. |
| | |
| If applicable Privacy Laws require a privacy notice to be given to Information Subjects, such notice must be developed in consultation with the respective Privacy Professional to ensure it includes all necessary information and is delivered to the Information Subject within the timeframe required by applicable Privacy Laws. | Ако приложимото Законодателство за неприкосновеност на Личните данни изисква Субектът на данни да получи такова уведомление, уведомлението трябва да се изготви в консултация със съответния Специалист по неприкосновеност на Личните данни, за да се гарантира, че то включва цялата необходима информация и е доставено на Субекта на данни в сроковете, определени от това законодателство. |
| | |
| When an Information Subject inquires with the Company about their Personal Information, or otherwise seeks to exercise any related rights, the Employee receiving the inquiry must promptly notify the Privacy Liaison for the respective Business Function. The Privacy Liaison must verify the identity of the requestor and refer the inquiry to the respective Privacy Professional for handling. | В случай, че Субект на Лични данни подаде запитване към Компанията относно Личните си данни или по друг начин търси да упражни правата си, Работодателят който е получил такова запитване е длъжен своевременно да уведоми Лице за контакт в съответната Бизнес функция. Съответното Лице за контакт по отношение на Личните данни трябва да потвърди идентификацията на заявителя и да препрати запитването към съответния Специалист по неприкосновеност на Личните данни. |
| | |
| ## 4.7 Transfer Limitation | ## 4.7 Ограничения за предаване на данни |
| | |
| The Company may engage Third-Parties Processors for various services, such as hosting and storage cloud computing, contract management, background and due diligence screening, reporting and assurance, risk analysis and mitigation, payroll and benefits management, as well as speak-up and incident reporting services. | Компанията може да ангажира обработващи Трети страни за изпълнение на различни услуги като например облак /хоустинг, съхранение и компютърна обработка, управление на договори, дю дилижънс и проверка на факти, изготвяне на отчети и проверка на качество, анализ и намаляване на риска, управление на заплати, осигуровки и социални придобивки, а също и процеса по сигнализиране на нередности. |
| | |

| | |
|---|---|
| When engaging Third Party Processors, the Company remains accountable for the Personal Information Processed by these entities. Therefore, a Data Processing Agreement must be entered into before any transfer of Personal Information occurs. Privacy Liaisons are accountable for ensuring that a Data Processing Agreement is in place, in consultation with the IT Privacy Coordinator and the respective Privacy Professional. | При ангажиране на обработваща Трета страна, Компанията продължава да носи отговорност за обработването на Личните данни. В този смисъл, Компанията трябва да сключи с такава страна Споразумение за обработка на Лични данни преди обработването на каквато и да е Лична информация от тази трета страна да е започнало. Лицето за контакт по отношение на Личните данни носи отговорност за това да има сключено Споразумение за обработка на Лични данни, и това споразумение да е изготвено в консултация с ИТ Координатор за Лични данни и съответния Специалист по неприкосновеност на Личните данни. |
| | |
| The Data Processing Agreement must require the Third Party to adhere to the relevant Company Policy Documents related to the protection of Personal Information, unless the Privacy Professional determines that the Third-Party Processor has its own policy documents consistent with the principles set out in this Standard. | Споразумението за обработка на Лични данни трябва да има клауза, изискваща от Третата страна да спазва съответните Политики на Компанията, свързани с Личните данни, освен ако Специалистът по неприкосновеност на данните потвърди, че Третата страна има собствени политики/ документи, които отговарят на принципите в настоящия Стандарт. |
| | |
| Additionally, the Data Processing Agreement must clearly define the scope of the Third-Party Processor's activities, stipulating that Processing may not be undertaken for any other purpose. | Освен това, Споразумението за обработка на данни трябва ясно да задава обхвата на дейностите на Третата страна и задължението ѝ да не използват данните за други цели. |
| | |
| Privacy Liaisons must assess whether Processing of Personal Information by their respective Business Functions will involve transferring Personal Information outside of the country of Collection. Since Privacy Laws may restrict such transfers to certain jurisdictions, the respective Business Unit's Privacy Professional must be notified before any transfer occurs to evaluate potential restrictions. | Лицата за контакт трябва да преценят дали обработката на Лични данни от съответната Бизнес функция ще включва прехвърляне на Лични данни извън държавата, в която са събрани. Тъй като в някои юрисдикции Законодателството за неприкосновеност на Личните данни може да налага ограничения на такова прехвърляне, Специалистът по неприкосновеност на данните в дадената Бизнес единица трябва да бъде уведомен преди такова прехвърляне на данни, за да провери дали има такива ограничения. |
| | |
| ## 4.8 Confidentiality and Authorization | ## 4.8 Конфиденциалност и оторизации |
| | |
| Only authorized Employees are permitted to engage in the Processing of Personal Information. These Employees are strictly prohibited from using such Personal Information for personal purposes, transferring it or making it accessible in any manner to unauthorized Employees, Third Parties or any other external stakeholder. Within the context of this Standard, "unauthorized" also refers to the use of Personal Information by Employees for purposes unrelated to their employment duties. | Лични данни се обработват само от оторизиран персонал. За тези работници/служители важи стриктна забрана да използват Лични данни за лични цели, и да ги прехвърлят или да предоставят достъп до тях на неоторизиран персонал на Компанията, на Трети страни или други външни заинтересовани страни. В контекстна на настоящия Стандарт, "неоторизиран" се отнася и за използването на Лични данни от страна на работници/служители за цели, които не са свързани с трудовите им задължения. |
| | |

| 4.9 Reporting Personal Information Breaches | 4.9 Докладване на случаи на неоторизирано разкриване на Лични данни |
|---|---|
| | |
| Preventing Personal Information Breaches is the accountability of all Employees and Third Parties. All actual or suspected Personal Information Breaches must be reported immediately to a Privacy Liaison or to the Privacy Professional of the respective Business Unit. | Работниците/служителите носят отговорност за предотвратяване на такова неоторизирано разкриване на Лични данни Всички инциденти с неоторизирано разкриване на Лични данни (действително или предполагаемо) задължително и незабавно се докладват на Лицето за контакт по отношение на Личните данни в съответната Бизнес единица. |
| | |
| In the event of a Personal Information Breach, Privacy Professionals will coordinate an investigation in close collaboration with the IT Privacy Coordinator. The Company will promptly take steps to contain and assess the breach, ensuring that measures are implemented to minimize harm. Depending on the nature of the Personal Information Breach, affected Information Subjects and relevant regulatory authorities may need to be notified. | При неоторизирано разкриване на Лични данни, Специалистите по неприкосновеност координират разследването в тясно сътрудничество с ИТ Координатор за Лични данни. В такъв случай Компанията предприема навременни мерки за контрол и оценка на такъв неоторизиран достъп и прилага мерки за минимизиране на последиците. В зависимост от характера на този инцидент, може да се наложи уведомяване на засегнатите Субекти на Лични данни и съответните институции. |
| | |
| 4.10 Data Protection Measures and Privacy by Design | 4.10 Мерки за защита и неприкосновеност, заложени в системата |
| | |
| To safeguard the confidentiality, integrity and security of the Personal Information it Collects, the Company, with the support of the IT Department, must implement physical, technical and administrative security measures. Examples of these measures are provided in Appendix A. | С помощта на ИТ Отдела, Компанията трябва да внедрява физически, технически и административни мерки за защита на конфиденциалността, интегритета и сигурността на събираните от нея Лични данни. В Приложение А са дадени примери за такива мерки. |
| | |
| When implementing new applications and services, the Company is committed to embedding privacy into their design and operation from the outset, adhering to the principle of "privacy by design". | При внедряване на нови приложения и услуги, Компанията от самото начало залага защита на данните в структурата и функционалните им характеристики на принципа "неприкосновеност по дизайн (privacy by design)". |
| | |
| 4.11 Privacy Impact Assessment and Risk | 4.11 Оценка на въздействието и риска върху неприкосновеността на данните |
| | |
| To uphold its commitment to protecting Personal Information and to enable transparency and control, the Company will conduct “Privacy Impact Assessments” where appropriate. A Privacy Impact Assessment is a systematic process designed to evaluate how Personal Information is Collected, used, disclosed and managed | За изпълнение на ангажиментите си за защита на Личните данни и за осигуряване на прозрачност и контрол, когато е необходимо, Компанията провежда “Оценка на въздействието върху неприкосновеността”. Оценката на въздействието върху неприкосновеността представлява систематичен |

| | |
|---|---|
| within the Company's operations. This process helps the Company identify potential Privacy risks and implement measures to mitigate them, especially when introducing new technologies, systems, or processes that involve Personal Information. | процес, с който се оценява как Личните данни се събират, разкриват и управляват при дейността на Компанията. Този процес помага на Компанията да идентифицира рискове за неприкосновеността на Личните данни и да внедрява мерки за намаляването на тези рискове, особено при въвеждане на нови технологии, системи и процеси, които включват Лични данни. |
| | |
| The Company will conduct Privacy Impact Assessments in the following scenarios: | Компанията провежда Оценка на въздействието върху неприкосновеността в следните случаи: |
| | |
| • When new projects or systems are introduced that Collect or otherwise Process Personal Information; | • Когато се въвеждат нови проекти и системи, при които се събират или по друг начин се обработват Лични данни; |
| • When existing Processing activities undergo significant changes; and | • Когато се правят съществени промени в съществуващите дейности по обработка; и |
| • When legal requirements mandate such assessment (e.g., in response to regulatory changes). | • Когато нормативните / юридически изисквания налагат такава оценка (напр. при промени в нормативни документи). |
| | |
| Privacy Impact Assessments are carried out by the respective Privacy Liaisons under the oversight of the respective Privacy Professionals and in consultation with the IT Privacy Coordinator and the Group Privacy Officer, when necessary. | Оценка на въздействието върху неприкосновеността се извършва от съответното Лице за контакт по отношение на Личните данни под контрола на Специалист по неприкосновеност на Личните данни и в консултация с ИТ Координатор за Лични данни и Отговорника за Лични данни в Групата ДПМ, когато е необходимо. |
| | |
| ## 4.12 Mobile Device, Email and Internet Usage | ## 4.12 Използване на мобилни устройства, и-мейл и интернет |
| | |
| Employees must exercise special caution when sharing or otherwise Processing Personal Information via mobile devices such as smartphones, tablets and notebooks as well as through email and internet use. Detailed requirements can be found in the *Acceptable Mobile Device Use Procedure, Acceptable Email Use Procedure* and the *Internet Acceptable Use Procedure*. | Работниците/служителите трябва да са особено предпазливи при споделяне или обработка на Лични данни чрез мобилни устройства като смарт телефон, таблет и ноутбук, а също и такива, които се обменят по и-мейл и интернет. Изискванията са описани подробно в *Процедура за допустима употреба на мобилните устройства, Процедура за допустимо използване на електронна поща* и *Процедура за допустима употреба на Интернет.* |
| | |
| # 5 Role Relationships, Authorities and Accountabilities | # 5 Взаимодействие между ролите, правомощията и отговорностите |
| | |
| To facilitate compliance with this Standard, certain roles, relationships, and accountabilities are prescribed herein. | За спазване на настоящия Стандарт, тук са препоръчани определени роли, правоотношения и отговорности |
| | |

| 5.1 Group Privacy Officer | 5.1 Отговорник за Лични данни в Групата ДПМ |
|---|---|
| The Group Privacy Officer is accountable for overseeing compliance with this Standard, and reporting to DPMs senior management, with the support of designated Privacy Professionals. To fulfill these accountabilities, the Group Privacy Officer may request information from the Privacy Professionals, who are obligated to provide the requested information within a reasonable timeframe. | Отговорникът за Лични данни в Групата на ДПМ носи отговорност за контрола върху спазването на настоящия Стандарт и свързаната с това отчетност пред Висшето ръководство, с помощта на Специалистите по неприкосновеност на Личните данни. За изпълнението на тези отговорности, Отговорникът за Лични данни в Групата на ДПМ може в разумни срокове да иска информация от Специалистите по неприкосновеност на Личните данни. |
| In the absence of a designated Privacy Professional for DPM, the accountabilities outlined in Section 5.2 below will be assumed by the Group Privacy Officer | Ако не са определени Специалисти по неприкосновеност на Личните данни, отговорностите в Раздел 5.2 долу се възлагат на Отговорника за Лични данни в Групата ДПМ. |
| **5.2 Privacy Professionals** | **5.2 Специалисти по неприкосновеност на Личните данни** |
| Privacy Professionals are accountable for ensuring that applicable Privacy Laws are understood, communicated and integrated into the practices of their respective Business Unit. | Специалистите по неприкосновеност на Личните данни носят отговорност за осигуряване на разбирането, комуникирането и интегрирането на приложимите нормативни изисквания за Личните данни в практиките на съответната Бизнес единица. |
| The key accountabilities of Privacy Professionals include, but are not limited to: | Основните отговорности на Специалиста по неприкосновеност на Личните данни включват, но не се ограничават до следното: |
| • Maintaining up-to-date knowledge of applicable Privacy Laws and notifying Group Privacy Officer of any significant changes; | • Поддържа актуална информация за нормативните изисквания, приложими към неприкосновеността на Личните данни, и уведомява Отговорника за Лични данни в Групата при съществени промени в тях; |
| • Developing and updating Privacy policy documents for their respective Business Unit; | • Изготвя и актуализира документи, свързани с Политиките за неприкосновеност на Личните данни за съответната Бизнес единица; |
| • Creating and delivering Privacy training programs for Employees for their respective Business Unit; | • Разработва и провежда обучителни програми във връзка с неприкосновеност на Личните данни за персонала в съответната Бизнес единица; |
| • Assisting and advising Privacy Liaisons in establishing Data Processing Agreements when engaging Third Party Processors; | • Подпомага и консултира Лицата за контакт по отношение на Личните данни при сключване на Споразумения за обработка на Лични данни, в които са ангажирани Трети страни, които обработват Лични данни; |

| | |
|---|---|
| • Notifying the Group Privacy Officer of any Privacy Data Breaches and coordinating the investigation and response to such beaches; | • Уведомява Отговорника за Лични данни в Групата на ДПМ при нарушение на сигурността на данните и координира разследвания и последващите действия при такива нарушения; |
| • Overseeing Privacy Impact Assessments conducted by Privacy Liaisons within their respective Business Unit; and | • Контролира Оценката на въздействието върху неприкосновеността на данните, която се изготвя от Лицата за контакт по отношение на Личните данни в съответната Бизнес единица; и |
| • Acting as the primary point of contact with Privacy authorities for their respective Business Units. | • Функционира като основно лице за контакт между съответната Бизнес единица и институциите за защита на Личните данни. |
| | |
| ## 5.3 Privacy Liaison | ## 5.3 Лице за контакт по отношение на Личните данни |
| | |
| Each Business Function Head whose Business Functions Processes Personal Information, must designate an Employee within the Business Function to serve as a Privacy Liaison and facilitate the adherence to this Standard. | Всеки ръководител на Бизнес функция в която се обработват Лични данни е длъжен да определи един служител в тази Бизнес функция, който да играе роля на Лице за контакт по отношение на Личните данни и да подпомага спазването на настоящия Стандарт. |
| | |
| The key accountabilities of the Privacy Liaisons include, but are not limited to: | Основните отговорности на Лице за контакт по отношение на Личните данни включват, но не се ограничават до следното: |
| • Ensuring that Privacy considerations are integrated into the business processes and projects of their respective Business Function; | • Следи за това неприкосновеността на Личните данни да е интегрирана в бизнес процесите и проектите на съответната Бизнес функция. |
| • Ensuring that Personal Information Processed by their respective Business Function is collected, used and stored in compliance with this Standard; | • Осигурява спазване на настоящия Стандарт при събиране, ползване и съхранение на Личните данни в съответната Бизнес единица; |
| • Ensuring a Data Processing Agreement is executed after consulting the respective Business Unit's Privacy Professional and the IT Privacy Coordinator; | • Осигурява сключване на Споразумение за обработка на Лични данни след консултации със съответния Специалист по неприкосновеност на Личните данни и ИТ Координатор за Лични данни. |
| • Reporting privacy concerns and Personal Information Breaches to the Privacy Professionals; and | • Докладва на Специалистите по неприкосновеност проблеми със защитата или нарушение на сигурността на Личните данни; и |
| • Conducting Privacy Impact Assessments, as required. | • Изготвя Оценки на въздействието върху неприкосновеността на данните, когато е необходимо. |
| | |

| 5.4 IT Privacy Coordinator | 5.4 ИТ Координатор за Лични данни |
|---|---|
| The IT Privacy Coordinator is accountable for supporting the Group Privacy Officer and Privacy Professionals and ensuring the implementation of the Company technological controls designed to protect Personal Information. | ИТ Координаторът за Лични данни съдейства на Отговорникът за Лични данни в Групата на ДПМ и Специалистите по неприкосновеност на Личните данни за внедряването на технологични контролни мерки за защита на Личните данни. |
| The key accountabilities of the IT Privacy Coordinator include, but are not limited to: | Основните отговорности на ИТ Координатор за Лични данни включват, но не се ограничават до следното: |
| • Reviewing, managing, and conducting regular testing and assessments to evaluate the effectiveness of technical and organizational measures for ensuring the security of Personal Information. | • Преглежда, управлява и провежда редовни тестове и оценка на ефективността на техническите и организационни мерки за сигурността на Личните данни. |
| • Assisting Privacy Professionals in responding to Information Subject requests or requests from Privacy authorities within the timeframes prescribed by Privacy Laws. | • Подпомага Специалистите по неприкосновеност на Личните данни в отговорите на запитвания от страна на Субекти на данни и институции за защита на Личните данни в сроковете, определени от съответните нормативни документи. |
| • Reviewing data security documents to ensure appropriate security controls, both prior to the onboarding of Third Party – Processors and as part of ongoing interactions with them. | • На текуща база, във взаимодействие с Трети страни, преглежда документите за сигурност на данните и осигурява подходящи контролни мерки за сигурност преди и след включването на Трети страни в обработката на данни. |
| • Assisting in identifying, managing and mitigating Personal Information Breaches through technological support. | • Подпомага, идентифицира, управлява и намалява рисковете за нарушение на сигурността на Личните данни с помощта на специалисти по технологии. |
| • Supporting Privacy Professionals in the execution of other accountabilities set out in this Standard, as needed. | • Където е необходимо, подпомага Специалистите по неприкосновеност на Личните данни за изпълнението на други задължения, описани в настоящия Стандарт. |
| **6 Effective Date and Review** | **6 Влизане в сила и прегледи на Стандарта** |
| | |
| This Standard must be reviewed once every two years. | Настоящият Стандарт се преразглежда веднъж на всеки две години. |
| | |
| **7 Compliance** | **7 Съответствие** |
| | |
| Any violation of this Standard must be reported through the speak-up channels specified in the *Code of Business Conduct and Ethics*. | Всяко нарушение на настоящия Стандарт задължително се докладва по каналите за докладване на нередности съгласно *Правилника за бизнес поведение и етика.* |
| | |
| Non-compliance with this Standard may subject a person to whom this Standard applies to corrective action by the Company as described in the *Code of Business Conduct and Ethics.* | Неспазването на настоящия Стандарт от страна на член на Борда на директорите, работник/служител или Трета страна подлежи на корективни мерки съгласно *Правилника за бизнес етика и поведение*. |
| | |

| 8 Appendices | 8 Приложения |
|---|---|
| | |
| Appendix A: Examples of Safeguard Measures | Приложение А: Примерни мерки за защита |

| Appendix A: Examples of Safeguard Measures | Приложение А: Примерни мерки за защита |
|---|---|
| | |
| **(a) Physical Security Measures** | **(а) Физически мерки за сигурност** |
| These measures protect the physical locations and devices where Personal Information is stored or accessed. Some examples include: | Представляват мерки за защита на физическото местоположение и устройствата за съхранение на и достъп до Лични данни. Някои от примерите включват: |
| • **Controlled Access to Facilities**: Only authorized Employees may access the Company's buildings or areas where Personal Information is stored. | • **Контролиран достъп до помещения**: Само оторизирани лица мога да влизат в сградите и зоните, в които се съхраняват Лични данни. |
| • **Secure Storage**: Hard copies of Personal Information (e.g., employee records, contracts) must be kept in locked cabinets, safes, or secure filing rooms that are only accessible to authorized Employees. | • **Защитено място за съхранение:** Разпечатките с Лични данни (например досиета и договори на работници/служители в "Личен състав") задължително се държат в заключени шкафове, сейфове или стаи, до които имат достъп само оторизирани служители. |
| • **Environmental Controls**: Protecting server rooms from environmental risks such as fire, floods, or overheating by using climate control, fire suppression systems, and uninterruptible power supplies. | • **Контрол върху средата:** Защита на сървърните помещения от рискове като пожар, наводнение и прегряване с помощта на климатици, противопожарни системи и UPS устройства за осигуряване на непрекъснато ел. захранване. |
| • **Visitor Control**: Implementing a strict visitor management system, including strict visitor protocols in secure areas. | • **Контрол на достъпа на посетители:** Включва скритна система за контрол на достъпа, включително стриктни правила за допускане на посетители в охранявани зони. |
| The Company may also adopt surveillance and monitoring techniques (such as the use of CCTV cameras and alarms to monitor access to facilities, data centers, and sensitive areas) after consulting with the Group Privacy Professional. | Освен това, Компанията може да въведе физически системи за наблюдение и мониторинг (видеокамери и аларми за наблюдение на помещения, зони за съхранение на данни и чувствителни зони) след консултиране със Специалиста по неприкосновеност на Личните данни за Групата на ДПМ. |
| | |
| **(b) Technical Security Measures** | **(b) Технически мерки за сигурност** |
| These are measures designed to protect digital systems and networks from cyber threats and unauthorized access. Some specific examples include: | Представляват мерки за защита на дигиталните системи и мрежи от кибер заплахи и неоторизиран достъп. Някои конкретни примери включват: |
| • **Data Encryption**: Encrypting sensitive Personal Information both at rest (in storage) and in transit (when being transmitted over networks) to prevent unauthorized access. | • **Криптиране на данни:** Представлява криптиране на Лични данни на мястото им за съхранение или на път (когато се прехвърлят по мрежи) с цел да се предотврати неоторизиран достъп. |

| | |
|---|---|
| • **Firewalls and Intrusion Detection Systems**: Using firewalls and intrusion detection/prevention systems to monitor and filter network traffic | • **Файъруол и системи за засичане на опити за неоторизиран достъп**: Използват се системи за защита тип Firewall**,** и системи за засичане/предотвратяване на неоторизиран достъп и мониторинг на мрежов трафик. |
| • **Multi-Factor Authentication:** Requiring multiple forms of verification for accessing sensitive systems or information. | • **Многофакторна автентикация:** Изисква няколко типа верификация за достъп до системи с чувствителна информация. |
| • **Role-Based Access Controls**: Limiting access to Personal Information based on an Employee's role or job accountabilities. | • **Контрол на достъпа, базиран на роли (RBAC):** Ограничава достъпа до Лични данни на база на ролите и отговорностите на съответния работник/служител. |
| • **Regular Security Audits and Vulnerability Assessments**: Regularly assessing and testing the company's IT infrastructure to identify and address potential treats. | • **Редовни одити на сигурността и Оценка на уязвимостта:** Редовни оценки и тестване на ИТ инфраструктурата на компанията за идентифициране и адресиране на потенциалните заплахи. |
| • **Anti-virus and Anti-malware Software**: Deploying and regularly updating anti-virus and anti-malware software on all Company systems to detect and remove malicious software. | • **Софтуер за защита срещу вируси и малуер**: Инсталиране и редовен ъпдейт на антивирусния и антималуер софтуер на всички системи в компанията с цел засичане и премахване на зловреден софтуер. |
| • **Backup Systems**: Implementing automatic backups of important information, stored in secure, off-site locations or in the cloud. | • **Бекъп системи:** Внедряване на автоматични системи за бекъп на важна информация, която се съхранява на защитени устройства в облак или извън територията на компанията. |
| • **Web filtering:** Blocking access to malicious and unauthorized websites, reducing the risk of malware, phishing, and data breaches. | • **Филтриране на достъпа до интернет сайтове:** Блокиране на достъпа до зловредни и неоторизирани уебсайтове, намаляване на риска от фишинг атаки и неоторизиран достъп до данни. |
| • **Patch Management**: Regularly updating software with the latest security software updates (i.e. patches) to mitigate vulnerabilities. | • **Управление на актуализации**: Редовен ъпдейт на софтуер с последните актуализации на софтуер за сигурност (patches) за намаляване на уязвимостта. |
| • **Security Incident and Event Management**: Implementing tools, which provide centralized monitoring, analysis, and real-time alerting of security events across the Company's network. | • **Управление на инциденти със сигурността:** Внедряване на инструменти за централизиран мониторинг, анализ и сигнализиране на опасности и проблеми в реално време за събития в цялата мрежа на компанията. |
| • **Security Incident Response Plan:** Quickly identifying and mitigating security breaches to minimize damage and information loss | • **План за действия при инциденти със сигурността:** Спешно идентифициране и намаляване на броя на проблемите/инцидентите със сигурността за минимизиране на щетите и загубата на информация. |
| • **Disaster Recovery Plan:** Focusing on restoring IT systems and information access after disruptions to ensure business continuity. | • **План за възстановяване при бедствия и аварии:** Планът се фокусира върху възстановяване на достъпа до ИТ системи и |

| | |
|---|---|
| | информация след прекъсване на услугите, за да се осигури непрекъснатост на бизнеса. |
| | |
| **(c) Administrative Security Measures** | **(c) Административни мерки за сигурност** |
| Administrative measures ensure that policies, procedures, and employee behavior contribute to the protection of Personal Information. These include: | Административните мерки подпомагат политиките, процедурите и поведението на персонала, така че да се осигури защита на Личните данни. Административните мерки включват: |
| • **Privacy Policies and Procedures**: Developing and communicating clear policies for handling, access, retention, and deletion of Personal Information. | • **Политики и процедури за неприкосновеност на Личните данни:** Разработване и комуникиране на ясни политики за обработка, достъп, съхранение и изтриване на Лични данни. |
| • **Employee Training and Awareness**: Providing regular training to Employees on best practices for data security, phishing awareness, password management, and how to report suspicious activity. | • **Обучение и информираност на персонала:** Осигуряване на редовно обучение на персонала за използване на добри практики за защита на данните, разпознаване на фишинг атаки, управление на пароли и методи за докладване на съмнителни действия. |
| • **Third-Party Processor Vendor Management**: Ensuring that Third-Party Processors comply with the Company's privacy and security standards. | • **Управление на Трети страни, които обработват Лични данни:** Така се осигурява спазване на изискванията за сигурност и неприкосновеност на Личните данни от страна на Трети страни. |
| • **Regular Audits and Compliance Checks**: Conducting internal and external audits to ensure compliance with Privacy Laws and Company policies. | • **Редовни одити и проверки за спазване на изискванията:** Провеждане на вътрешни и външни одити за съответствие с нормативните изисквания за неприконовеност на Личните данни и политиките на компанията. |