سياسة خصوصية البيانات

Data Privacy Policy

مكتب خصوصية البيانات

Data Privacy Office

ديسمبر 2024

December 2024

التصنيف: سري

CLASSIFICATION: Confidential

Title	Data Privacy Policy	سياسة خصوصية البيانات	العنوان
Applies To	SALAMA Cooperative Insurance Co.	شركة سلامة للتأمين التعاوني	يطبق على
Issue Number	2	2	رقم الإصدار
Issue Date	October 2024	أكتوبر 2024	تاريخ الإصدار
Effective Date	December 2024	ديسمبر 2024	تاريخ التطبيق
Revision Date	December 2024	ديسمبر 2024	تاريخ المراجعة
Number Of Pages	27	27	عدد الصفحات

المادة قبل التعديل	المادة بعد التعديل	رقم المادة/ رقم الصفحة
Salama Data Privacy Policy	DPO_Data Privacy Policy_Final2024	**التحسين الشامل وفقاً لنظام حماية البيانات الشخصية**

Definition

Consent: A knowing, voluntary, clear, and specific, expression of consent, whether oral or written, from the Data Subject signifying agreement to the processing of their Personal Data

Child: Any person under 18 years of age.

Data Controller: Any entity, or any natural or legal person, that collects Personal Data from a Data Subject and carries out processing of that Personal Data, directly or indirectly, through a processor, pursuant to a legal basis.

Data Processor: Any independent governmental or public entity, or any natural or legal person, which engages in the processing of Personal Data, on behalf of a Data Controller pursuant to a legal basis.

Data Protection Impact Assessments (DPIA): A process to systematically analyze, identify and minimize the data protection risks of a process or project.

Data Subject / Personal Data Owner: An individual to whom the Personal Data belongs, his representative, or whoever has legal guardianship over the Data Subject

Data Subject Rights: Any request received by SALAMA from a Data Subject or other individual or legal entity who wishes to receive a copy of all the Personal Data related to it or the Data Subject the firm is processing about them.

Disclosure of Personal Data: Enabling any person - other than the Controller or the Processor, as the case may be - to access, collect or use personal data by any means and for any purpose.

Guardian: Any person who is has been given the legal responsibility to care for a child or an adult who does not have the capacity for self-care or property

Implied Consent: Consent of the Data Subject that is understood from their actions, certain events, or circumstances.

Partner: An external organization with which SALAMA conducts business and is also authorized to, under the direct authority of SALAMA Process the Personal Data of SALAMA Data Subjects, Employees, Suppliers, Service Providers and Contractors etc.

Personal Data Breach: Disclosure, acquisition, or access to Personal Data in unauthorized form or in absence of a legal basis, whether intentionally or unintentionally

Personal Data Destruction: Any action that leads to removal of Personal Data, rendering it impossible to

التعريفات

الموافقة: موافقة تمنح بشكل مباشر من صاحب البيانات الشخصية بأي شكل من الأشكال (شفهية أو مكتوبة) وتدل على قبوله بمعالجة بياناته الشخصية بحيث لا يمكن تفسيرها بخلاف ذلك، وتكون قابلة للإثبات.

طفل: أي شخص أقل من 18 سنة.

جهة التحكم: أي جهة، أو أي شخص طبيعي أو اعتباري، يقوم بجمع البيانات الشخصية من صاحب البيانات الشخصية وينفذ معالجة تلك البيانات الشخصية، بشكل مباشر أو غير مباشر، من خلال معالج، وفقًا لأساس قانوني.

جهة المعالجة: أي جهة حكومية أو عامة مستقلة، أو أي شخصية طبيعية أو اعتبارية خاصة؛ تعالج البيانات الشخصية لمصلحة جهة التحكم ونيابًة عنها وفقًا لأساس قانوني.

تقييمات أثر حماية البيانات: تقييم أثر عمليات المعالجة على حماية البيانات الشخصية.

مالك/صاحب البيانات الشخصية: الشخص الذي تنتمي إليه البيانات الشخصية، أو ممثله القانوني، أو أي شخص لديه ولاية قانونية على صاحب البيانات الشخصية.

حقوق صاحب البيانات: أي طلب تتلقاه سلامة من صاحب البيانات الشخصية أو أي فرد أو كيان قانوني آخر يرغب في الحصول على نسخة من جميع المعلومات الشخصية المتعلقة به أو بصاحب البيانات الشخصية التي تعالجها الشركة عنه.

الافصاح عن البيانات الشخصية: الوصول المتعمد أو غير المتعمد للبيانات الشخصية من قبل أي جهة، بخلاف جهة التحكم، أو جهة المعالجة أو صاحب البيانات الشخصية، مما يتيح لهم استخدامها أو عرضها بأي وسيلة ولأي غرض.

الوصي: هو أي شخص تم تكليفه بالمسؤولية القانونية لرعاية طفل أو شخص بالغ ليس لديه القدرة على العناية بنفسه أو ممتلكاته.

الموافقة الضمنية: موافقة صاحب البيانات الشخصية التي تُفهم من أفعاله أو أحداث، أو ظروف معينة.

الشريك: منظمة خارجية تدير معها سلامة أعمالا وهي مخولة أيضا، تحت السلطة المباشرة من سلامة، بمعالجة البيانات الشخصية لأصحاب البيانات الشخصية لسلامة، والموظفين، والموردين، ومقدمي الخدمات، والمتعاقدين وما إلى ذلك.

تسرب البيانات الشخصية: أي حادثة تؤدي إلى الإفصاح عن البيانات الشخصية أو تلفها أو الوصول غير المشروع إليها، سواء كان ذلك بقصد أو بغير قصد، وبأي وسيلة كانت سواء آلية أو يدوية.

view such Personal Data or retrieve it by any means, whether digital or physical

Personal Data Processing: Processing of Personal Data by any means, whether manual or automated processing (digitally and non-digitally), including collection, transfer, recording, storage, data-sharing, destruction, analysis, extraction of their patterns, conclusion, and interconnection

Personal Data: Any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, addresses, contact numbers, license numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of personal nature.

Credit Data: Any Personal Data related to an individual's request for, or obtaining of, financing from a financing entity, whether for a personal or family purpose, including any data relating to that individual's ability to obtain and repay debts, and the credit history of that person.

Health Data: Any Personal Data related to an individual's health condition, whether their physical, mental or psychological conditions, or related to Health Services received by that individual.

Sensitive Data: Personal Data revealing racial or ethnic origin, or religious, intellectual or political belief, data relating to security criminal convictions and offenses, biometric or Genetic Data for the purpose of identifying the person, Health Data, and data that indicates that one or both individual's parents are unknown.

Privacy Assessments: A privacy assessment is a process for identifying and assessing privacy risks throughout the Personal Data life cycle of a program or system or applications.

Process Owners: A process owner is the person/ department solely responsible for owning a process. They are accountable for designing an effective and efficient process, using the right people and financial and technical resources to run the process, and delivering quality outcomes as required within SALAMA.

Implicit Consent: Consent that is not given Explicitly by the Data Subject or the authorized person but given implicitly through the person's actions and the facts and circumstances of the situation.

إتلاف البيانات الشخصية: أي إجراء يؤدي إلى إزالة البيانات الشخصية، مما يجعل من المستحيل عرض هذه البيانات الشخصية أو استرجاعها بأي وسيلة، سواء كانت رقمية أو مادية.

معالجة البيانات الشخصية: معالجة البيانات الشخصية بأي وسيلة، سواء كانت معالجة يدوية أو معالجة آلية (رقمية وغير رقمية)، بما في ذلك جمع البيانات، ونقلها، وتسجيلها، وتخزينها، ومشاركتها، وإتلافها، وتحليلها، واستخراج أنماطها، واستنتاجاتها، والربط بينها.

البيانات الشخصية: هي أي عنصر من عناصر البيانات، بغض النظر عن المصدر أو الصيغة أياً كانت، والتي يمكن أن تؤدي بشكل مستقل أو عند دمجها مع معلومات أخرى متاحة إلى تحديد هوية الشخص بما في ذلك على سبيل المثال لا الحصر: الاسم الأول واسم العائلة، وأرقام الهوية الوطنية (الإقامة، جواز السفر، إلخ)، العناوين، رقم الهاتف، رقم حساب شركة التأمين، رقم بطاقة الائتمان، البيانات الصحية، صور أو مقاطع فيديو للشخص.

البيانات الائتمانية: كل بيان شخصي يتعلق بطلب الفرد الحصول على تمويل، أو حصوله عليه، سواء لغرض شخصي أو عائلي، من جهة تُمارس التمويل، بما في ذلك أي بيان يتعلق بقدرته على الحصول على ائتمان أو بقدرته على الوفاء به أو بتاريخه الائتماني.

البيانات الصحية: كل بيان شخصي يتعلق بحالة الفرد الصحية، سواء الجسدية أو العقلية أو النفسية أو المتعلقة بالخدمات الصحية الخاصة به.

البيانات الحساسة: كل بيان شخصي يتعلق بأصل الفرد العرقي أو أصله الإثني، أو معتقده الديني أو الفكري أو السياسي. وكذلك البيانات الأمنية والجنائية، أو بيانات السمات الحيوية التي تحدد الهوية، أو البيانات الوراثية، أو البيانات الصحية، والبيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهما.

تقييمات الخصوصية: تقييم الخصوصية هو عملية لتحديد وتقييم مخاطر الخصوصية طوال دورة حياة البيانات الشخصية لبرنامج أو نظام أو تطبيقات.

مالك العملية: مالك العملية هو الشخص/القسم المسؤول الوحيد عن امتلاك العملية. ويكون مسؤولاً عن تصميم عملية فعالة وذات كفاءة، واستخدام الأشخاص المناسبين والموارد المالية والتقنية المناسبة لتشغيل العملية، وتقديم نتائج عالية الجودة على النحو المطلوب داخل المنظمة.

الموافقة الضمنية: الموافقة التي لا تُعطى بشكل صريح من قبل صاحب البيانات أو الشخص المخوّل، ولكنها تُعطى ضمنيًا من خلال تصرفات الشخص ووقائع وظروف الموقف.

Explicit Consent: Direct and explicit consent given by the Data Subject in any form that clearly indicates the Data Subject's acceptance of the Processing of their Personal Data in a manner that cannot be interpreted otherwise, and whose obtention can be proven.

Transfer: Transferring Personal Data from one location to another in order to process it through some communication methods (including internal and external transfer in SALAMA, KSA)

Third party: A third party is an individual or any business entity that has a relationship with SALAMA to provide products or services directly to SALAMA or its customers on behalf of SALAMA. Third party is an acceptable umbrella term for a vendor, supplier, provider, broker etc.

الموافقة الصريحة: موافقة تمنح بشكل مباشر وصريح من صاحب البيانات الشخصية بأي شكل من الأشكال وتدل على قبوله بمعالجة بياناته الشخصية بحيث لا يمكن تفسيرها بخلاف ذلك، وتكون قابلة للإثبات.

النقل: نقل البيانات الشخصية من موقع إلى آخر من أجل معالجتها من خلال بعض وسائل الاتصال (بما في ذلك النقل الداخلي والخارجي في سلامة، أو في المملكة العربية السعودية)

الجهة / الطرف الثالث: الطرف الثالث هو فرد أو أي كيان تجاري له علاقة مع شركة سلامة لتقديم منتجات أو خدمات مباشرة إلى سلامة أو لعملائها نيابةً عنها. يعد مصطلح "الطرف الثالث" مصطلحًا شاملاً يشمل البائع والمورد والمزود، إلخ

1. Introduction

Salama Cooperative Insurance Company “SALAMA” is committed to protecting the Personal Data of its customers, employees, engaged third parties etc., while conducting its business in accordance with applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. This policy sets forth the expected behaviors of SALAMA employees and Third Parties in relation to the collection, usage, retention, transfer, disclosure, destruction, and breach of any Personal Data processed by SALAMA on behalf of an individual (i.e., the Data Subject).

Any breach of this policy will be taken seriously and may result in disciplinary action in accordance with SALAMA policies and procedures.

2. Purpose & Scope

2.1. Purpose

The purpose of this policy is to establish the essential principles and guidelines for the processing of Personal Data. It also indicates the key roles and responsibilities of business departments and employees while processing Personal Data to comply with Kingdom of Saudi Arabia laws and regulations related to Data Privacy and Personal Data Protection.

2.2. Policy Scope and Applicability

This policy applies to all processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files, hard copy that are structured in a way that allows access to information about individuals.

2.3. Ownership and policy Change Control

The Data Privacy Office at SALAMA cooperative owns this policy document, and will update this document based on the following:

Every time a legal or regulatory requirement change occurs to the policy.

1. المقدمة

تلتزم شركة سلامة للتأمين التعاوني "سلامة" بحماية البيانات الشخصية لعملائها وموظفيها والأطراف الثالثة المتعاقدة معهم وما إلى ذلك، أثناء إدارة أعمالها وفقًا لأنظمة ولوائح حماية البيانات المعمول بها وبما يتماشى مع أعلى معايير السلوك الأخلاقي. تحدد هذه السياسة السلوكيات المتوقعة من موظفي شركة سلامة والأطراف الثالثة فيما يتعلق بجمع أي بيانات شخصية تتم معالجتها من قبل شركة سلامة نيابةً عن فرد (أي صاحب البيانات) واستخدامها والاحتفاظ بها ونقلها والإفصاح عنها وإتلافها وخرقها.

سيؤخذ أي انتهاك لهذه السياسة على محمل الجد وقد يؤدي إلى اتخاذ إجراءات تأديبية وفقًا لسياسات وإجراءات سلامة.

2. الغرض والنطاق

2.1 الغرض

الغرض من هذه السياسة هو وضع المبادئ الأساسية والمبادئ التوجيهية لمعالجة البيانات الشخصية. بالإضافة إلى تحديد الأدوار والمسؤوليات الرئيسية لدوائر الأعمال والموظفين أثناء معالجة البيانات الشخصية للامتثال بما يمتثل بأنظمة المملكة العربية السعودية واللوائح المتعلقة بخصوصية البيانات وحماية البيانات الشخصية.

2.2 نطاق السياسة وقابلية تطبيقها

تنطبق هذه السياسة على جميع عمليات معالجة البيانات الشخصية التي تتم بصيغة إلكترونية (بما في ذلك البريد الإلكتروني والمستندات التي تم إنشاؤها باستخدام برامج معالجة النصوص) أو التي يتم الاحتفاظ بها في ملفات يدوية أو نسخ ورقية منظمة بطريقة تسمح بالوصول إلى المعلومات المتعلقة بالأفراد.

2.3 الملكية وضبط تغيير السياسة

يمتلك مكتب خصوصية البيانات في سلامة وثيقة السياسة هذه، وسيقوم بتحديث هذه الوثيقة بناءً على ما يلي:

في كل مرة يحدث فيها تغيير في المتطلبات القانونية أو التنظيمية للسياسة.

Management and other decision changes that may affect this document, whether directly or indirectly.

تغييرات الإدارة والقرارات الأخرى التي قد تؤثر على هذه الوثيقة، سواء بشكل مباشر أو غير مباشر.

At a minimum, this policy should be reviewed/updated annually.

كحد أدنى، يجب مراجعة/تحديث هذه السياسة سنويًا.

2.4. Applicable Laws and Regulatory Compliance Requirement

This policy adheres to the KSA Personal Data Protection Law and other relevant data management and data protection regulations, this has been designed to establish a baseline standard for the processing and protection of Personal Data by SALAMA.

Compliance to applicable laws and regulations shall be provided by the Compliance Department of SALAMA.

2.4 الأنظمة المعمول بها ومتطلبات الامتثال التنظيمي

تلتزم هذه السياسة بنظام حماية البيانات الشخصية في المملكة العربية السعودية وغيرها من لوائح إدارة البيانات وحماية البيانات ذات الصلة، وقد تم تصميم هذه السياسة لوضع معيار أساسي لمعالجة البيانات الشخصية وحمايتها من قبل شركة سلامة.

يتم توفير الامتثال للأنظمة واللوائح المعمول بها من قبل إدارة الامتثال والإلتزام في شركة سلامة.

2.5. Effective Date of Policy

The policy is effective from the date of its approval by Data Management Steering Committee.

2.5 تاريخ سريان السياسة

تسري السياسة من تاريخ اعتمادها من قبل اللجنة التوجيهية لإدارة البيانات.

3. Principles of Data Processing

SALAMA shall adheres to the following principles in day-to-day practices when processing Personal Data. These principles form the foundation of our data protection practices and are designed to ensure that Personal Data is handled legally, fairly, and transparently.

3. مبادئ معالجة البيانات الشخصية

يجب على شركة سلامة الإلتزام بالمبادئ التالية في الممارسات اليومية عند معالجة البيانات الشخصية. تشكل هذه المبادئ أساس ممارسات حماية البيانات لدينا، وهي مصممة لضمان التعامل مع البيانات الشخصية بشكل مشروع وعادل وبشفافية.

3.1. Lawfulness, Fairness, and Transparency

Personal Data shall be collected and processed lawfully, fairly, and transparently in relation to the data subject. This means that Personal Data collection and processing activities must have a valid legal basis, must be conducted in a way that respects the rights and interests of the data subject, and must be transparent so that data subjects understand how their data is being used. All Personal Data collection and processing activities must be reviewed to ensure they have a valid legal basis under the KSA PDPL. Privacy notice must be provided to data subjects to ensure transparency in data processing practices.

3.1 المشروعية والعدل والشفافية

يجب جمع البيانات الشخصية ومعالجتها بشكل نظامي وعادل وبشفافية فيما يتعلق بصاحب البيانات. وهذا يعني أن أنشطة جمع البيانات الشخصية ومعالجتها يجب أن يكون لها أساس قانوني سليم، ويجب أن تتم بطريقة تحترم حقوق ومصالح صاحب البيانات، ويجب أن تكون شفافة بحيث يفهم أصحاب البيانات كيفية استخدام بياناتهم. يجب مراجعة جميع أنشطة جمع البيانات الشخصية ومعالجتها للتأكد من أن لها أساسًا قانونيًا صالحًا بموجب نظام حماية البيانات الشخصية في المملكة العربية السعودية. كما يجب تقديم إشعار الخصوصية لأصحاب البيانات الشخصية لضمان الشفافية في ممارسات معالجة البيانات.

3.2. Purpose Limitation

Personal Data shall be collected for specified, explicit, and legitimate purposes and not further processed incompatible with those purposes. This ensures that Personal Data is only used for the purposes for which it was originally collected and that any further processing is aligned with those purposes.

All Personal Data collection activities must have clearly defined purposes that are communicated to data subjects at the time of collection. Any changes to the purposes of data processing must be documented and communicated to the data subjects.

3.3. Data Minimization

Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. This principle ensures that only the minimum amount of Personal Data necessary to achieve the processing purposes is collected and used.

Data collection forms and processes must be designed to collect only the Personal Data necessary for the specified purposes. Regular audits should be conducted to ensure compliance with the data minimization principle.

3.4. Accuracy

Personal Data shall be accurate and, where necessary, kept up to date. Inaccurate or outdated Personal Data must be corrected or deleted without delay. This principle ensures the integrity and reliability of Personal Data. Processes must be in place to regularly review and update Personal Data. Data subjects should be provided with the means to update their Personal Data or request corrections if inaccuracies are identified.

3.2 تقييد الغرض

يجب جمع البيانات الشخصية لأغراض محددة وصريحة ومشروعة وعدم معالجتها بشكل إضافي يتعارض مع تلك الأغراض. وهذا يضمن عدم استخدام البيانات الشخصية إلا للأغراض التي جُمعت من أجلها في الأصل، وأن أي معالجة أخرى تتوافق مع تلك الأغراض.

يجب أن يكون لجميع أنشطة جمع البيانات الشخصية أغراض محددة بوضوح ويتم إبلاغ أصحاب البيانات الشخصية بها وقت جمعها. يجب توثيق أي تغييرات تطرأ على أغراض معالجة البيانات وإبلاغ أصحاب البيانات الشخصية بها.

3.3 الحد الأدنى من البيانات الشخصية

يجب أن تكون البيانات الشخصية كافية وذات صلة ومقتصرة على ما هو ضروري فيما يتعلق بالأغراض التي تتم معالجتها من أجلها. يضمن هذا المبدأ جمع واستخدام الحد الأدنى فقط من البيانات الشخصية اللازمة لتحقيق أغراض المعالجة.

يجب أن تكون نماذج وعمليات جمع البيانات مصممة لجمع البيانات الشخصية الضرورية فقط للأغراض المحددة. يجب إجراء عمليات تدقيق منتظمة لضمان الامتثال لمبدأ التقليل من البيانات.

3.4 الدقة

يجب أن تكون البيانات الشخصية دقيقة ومحدثة عند الضرورة. يجب تصحيح البيانات الشخصية غير الدقيقة أو القديمة أو حذفها دون تأخير. يضمن هذا المبدأ سلامة البيانات الشخصية وموثوقيتها. يجب وضع عمليات لمراجعة البيانات الشخصية وتحديثها بانتظام. يجب تزويد أصحاب البيانات بالوسائل اللازمة لتحديث بياناتهم الشخصية أو طلب التصحيحات إذا تم تحديد معلومات غير دقيقة.

3.5. Storage Limitation

Personal Data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data is processed. Once the data is no longer needed, it must be securely deleted or destroyed as per the defined data retention schedules.

3.5 تقييد التخزين

يجب الاحتفاظ بالبيانات الشخصية في شكل يسمح بتحديد هوية أصحاب البيانات لمدة لا تزيد عن المدة اللازمة للأغراض التي تتم معالجة البيانات الشخصية من أجلها. بمجرد انتهاء الحاجة إلى تلك البيانات، يجب حذفها أو إتلافها بشكل آمن وفقًا للجداول الزمنية المحددة للاحتفاظ بالبيانات.

3.6. Integrity and Confidentiality

Personal Data shall be processed to ensure appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, tampering, modification, destruction, or damage, using appropriate technical or organizational measures.

IT and Cyber Security departments must implement robust security measures to protect Personal Data. This includes encryption, access controls, regular security assessments, and incident response protocols.

3.6 النزاهة والسرية

يجب أن تتم معالجة البيانات الشخصية لضمان الأمن المناسب، بما في ذلك الحماية من المعالجة غير المصرح بها أو غير القانونية ومن الفقدان العرضي أو التلاعب أو التعديل أو التدمير أو التلف، باستخدام التدابير التقنية أو التنظيمية المناسبة.

يجب على أقسام تكنولوجيا المعلومات والأمن السيبراني تنفيذ تدابير أمنية قوية لحماية البيانات الشخصية. ويشمل ذلك التشفير، وضوابط الوصول، وعمليات التقييم الأمني المنتظمة، وبروتوكولات الاستجابة للحوادث.

3.7. Accountability

SALAMA shall be responsible for and able to demonstrate compliance with these principles. This principle emphasizes the importance of being able to provide evidence of compliance with data protection laws and regulations.

The Data Privacy Office must maintain comprehensive records of all Personal Data processing activities, including data protection impact assessments (DPIAs), privacy notices, consent forms, and data breach reports. Regular audits should be conducted to ensure compliance and accountability.

3.7 المساءلة والمسؤولية

يجب أن تكون شركة سلامة مسؤولة وقادرة على إثبات الامتثال لهذه المبادئ. يؤكد هذا المبدأ على أهمية القدرة على تقديم دليل على الامتثال لأنظمة ولوائح حماية البيانات.

يجب أن يحتفظ مكتب خصوصية البيانات بسجلات شاملة لجميع أنشطة معالجة البيانات الشخصية (ROPAs)، بما في ذلك تقييمات تأثير حماية البيانات (DPIAs)، وإشعارات الخصوصية، ونماذج الموافقة، وتقارير انتهاكات البيانات. يجب إجراء عمليات تدقيق منتظمة لضمان الامتثال والمساءلة.

4. Legal Basis for Processing

Under the KSA PDPL, Personal Data must be processed based on one or more legal grounds. SALAMA recognizes the importance of establishing a valid legal

4. الأساس أو المسوغ القانوني للمعالجة

بموجب نظام حماية البيانات الشخصية في المملكة العربية السعودية، يجب معالجة البيانات الشخصية بناءً على أساس قانوني واحد أو أكثر. تدرك شركة

basis for all Personal Data processing activities. The following legal bases may be used:

سلامة أهمية إنشاء أساس قانوني صالح لجميع أنشطة معالجة البيانات الشخصية. يمكن اعتماد الأسس القانونية التالية:

4.1. Consent Based

Consent is one of the primary legal basis for processing Personal Data. Personal data can be processed with implicit consent. Explicit consent for automated decisions, sensitive and credit data or the explicit consent of a guardian in the case of children or individuals lacking legal capacity, is required before processing their Personal Data unless another legal basis applies. For example, consent might be necessary to send our marketing communications about available offers and services, and explicit to process a child's medical policy.

4.1 الموافقة

الموافقة هي أحد الأسس القانونية الأساسية لمعالجة البيانات الشخصية. يمكن معالجة البيانات الشخصية بموافقة ضمنية. ويُشترط الحصول على موافقة صريحة عند معالجة البيانات بإتخاذ قرارات مؤتمتة أو معالجة البيانات الحساسة أوالائتمانية كما يجب الحصول على الموافقة الصريحة من ولي الأمر في حالة الأطفال أو الأفراد الذين يفتقرون إلى الأهلية القانونية قبل معالجة بياناتهم الشخصية ما لم ينطبق أساس قانوني آخر. وعلى سبيل المثال، تكون الموافقة ضرورية لإرسال مراسلاتنا التسويقية حول العروض والخدمات المتاحة، أو الموافقة الصريحة لمعالجة السياسة الطبية للطفل.

4.2. Performance of Contract

Personal Data may be processed if it is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract. This legal basis applies when Personal Data processing is required to fulfill contractual obligations. Contracts and agreements with data subjects must have clearly outlined the purposes for which Data Subject Personal Data will be processed. Any Personal Data collected for the performance of a contract must be limited to what is necessary to fulfill the contractual obligations.

4.2 الالتزام بالتعاقد

قد تتم معالجة البيانات الشخصية إذا كان ذلك ضروريًا لتنفيذ عقد يكون صاحب البيانات طرفًا فيه، أو من أجل اتخاذ خطوات بناءً على طلب صاحب البيانات قبل إبرام العقد. ينطبق هذا الأساس القانوني عندما تكون معالجة البيانات الشخصية مطلوبة للوفاء بالالتزامات التعاقدية. يجب أن تكون العقود والاتفاقيات المبرمة مع أصحاب البيانات قد حددت بوضوح الأغراض التي ستتم من أجلها معالجة البيانات الشخصية لصاحب البيانات. يجب أن تقتصر أي بيانات شخصية يتم جمعها لتنفيذ العقد على ما هو ضروري للوفاء بالالتزامات التعاقدية.

4.3. Legal Obligation

Personal Data may be processed if it is necessary for compliance with a legal obligation to which the SALAMA is subject. This legal basis applies when the SALAMA is required to process Personal Data to comply with laws, regulations, or court orders.

SALAMA must identify and document all legal obligations that require the processing of Personal Data. Compliance with these obligations must be

4.3 الالتزام القانوني

قد تتم معالجة البيانات الشخصية إذا كان ذلك ضروريًا للامتثال لالتزام قانوني تخضع له شركة سلامة. ينطبق هذا الأساس القانوني عندما يُطلب من شركة سلامة معالجة البيانات الشخصية للامتثال للأنظمة أو اللوائح أو أحكام قضائية.

يجب على شركة سلامة تحديد وتوثيق جميع الالتزامات القانونية التي تتطلب معالجة البيانات الشخصية. يجب مراجعة الامتثال لهذه الالتزامات وتحديثها بانتظام لتعكس التغييرات في الأنظمة واللوائح.

regularly reviewed and updated to reflect changes in laws and regulations.

4.4. Vital Interests

Personal Data may be processed if it is necessary to protect the vital interests of the data subject or another natural person. This legal basis applies in situations where Personal Data processing is necessary to protect someone's life or health.

SALAMA must assess the necessity of processing Personal Data based on vital interests on a case-by-case basis. Data subjects should be informed of the processing as soon as possible, and the processing should be limited to what is necessary to protect their vital interests.

4.5. Legitimate Interests

Personal Data may be processed if it is necessary for the purposes of the legitimate interests pursued by the SALAMA or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This legal basis allows for flexibility in processing Personal Data for legitimate business purposes.

SALAMA must conduct a legitimate interest assessment (LIA) to balance the SALAMA's interests with the rights of the data subject. The LIA must be documented, and the processing must be limited to what is necessary to achieve legitimate interests.

5. Data Subject Rights

As per the PDPL Data Subjects have rights to exercise. SALAMA can follow the Data Subject Rights Procedure and committed to execute the below rights applicable to Data Subjects:

4.4 المصلحة الحيوية

قد تتم معالجة البيانات الشخصية إذا كان ذلك ضروريًا لحماية المصالح الحيوية لصاحب البيانات أو لشخص آخر. ينطبق هذا الأساس القانوني في الحالات التي تكون فيها معالجة البيانات الشخصية ضرورية لحماية حياة أو صحة شخص ما.

يجب على شركة سلامة تقييم ضرورة معالجة البيانات الشخصية بناءً على المصالح الحيوية على أساس كل حالة على حدة. يجب إبلاغ أصحاب البيانات الشخصية بالمعالجة في أقرب وقت ممكن، ويجب أن تقتصر المعالجة على ما هو ضروري لحماية مصالحهم الحيوية.

4.5 المصلحة المشروعة

قد تتم معالجة البيانات الشخصية إذا كان ذلك ضروريًا لأغراض المصالح المشروعة التي تسعى إليها شركة سلامة أو طرف ثالث، باستثناء الحالات التي يتم فيها تجاوز هذه المصالح من خلال المصالح أو الحقوق والحريات الأساسية لصاحب البيانات. يسمح هذا الأساس القانوني بالمرونة في معالجة البيانات الشخصية لأغراض تجارية مشروعة.

يجب على شركة سلامة إجراء تقييم للمصالح المشروعة (LIA) لتحقيق التوازن بين مصالح شركة سلامة وحقوق صاحب البيانات. يجب توثيق تقييم المصلحة المشروعة، ويجب أن تقتصر المعالجة على ما هو ضروري لتحقيق المصالح المشروعة.

5. حقوق أصحاب البيانات الشخصية

وفقًا لنظام حماية البيانات الشخصية (PDPL) يتمتع أصحاب البيانات بحقوق ممارسة. يمكن لسلامة اتباع إجراءات حقوق صاحب البيانات والالتزام بتنفيذ الحقوق التالية المطبقة على أصحاب البيانات:

Type of Requests	Description
The Right to Be Informed	Data Subjects have the right to be informed about the collection and use of their Personal Data, including the purposes of the data processing, the legal basis for processing, and the rights of the data subject. SALAMA must ensure that data subjects are provided with clear and accessible information, typically through privacy notices or similar means. If Personal Data is collected from third parties, SALAMA shall notify the data subject within 30 days. A more detailed explanation of the legal basis for processing shall also be provided, specifying when consent is optional or mandatory.
The Right to Access Personal Data	Data Subjects have the right to request and obtain access to their Personal Data held by SALAMA. This includes the right to know whether their data is being processed and to receive a copy of their Personal. SALAMA must provide a process for data subjects to submit access requests, and these requests must be fulfilled within the time limits specified by the PDPL.
The Right to Request Access to Personal Data	Data Subjects have the right to request that their Personal Data be provided in a structured, commonly used, and readable format. SALAMA must ensure that Personal Data is provided in a format that allows the data subject to reuse it or transmit it to another data controller. If the request is made repeatedly and requires unreasonably extraordinary efforts by SALAMA, therefore, SALAMA may request

نوع الطلب	الوصف
حق العلم	يحق لأصحاب البيانات أن يكونوا على علم بجمع بياناتهم الشخصية واستخدامها، بما في ذلك أغراض معالجة البيانات، والأساس القانوني للمعالجة، وحقوق صاحب البيانات. يجب أن تضمن شركة سلامة تزويد أصحاب البيانات بمعلومات واضحة ويمكن الوصول إليها، عادةً من خلال إشعارات الخصوصية أو وسائل مماثلة. إذا تم جمع البيانات الشخصية من أطراف ثالثة، يجب على شركة سلامة إخطار صاحب البيانات في غضون 30 يومًا. كما يجب تقديم شرح أكثر تفصيلاً للأساس القانوني للمعالجة، مع تحديد متى تكون الموافقة اختيارية أو إلزامية.
حق الوصول إلى البيانات الشخصية	يحق لأصحاب البيانات طلب الوصول إلى بياناتهم الشخصية التي تحتفظ بها شركة سلامة والحصول عليها. ويشمل ذلك الحق في معرفة ما إذا كانت بياناتهم قيد المعالجة والحصول على نسخة من بياناتهم الشخصية. يجب على شركة سلامة توفير عملية لأصحاب البيانات لتقديم طلبات الوصول، ويجب تلبية هذه الطلبات في غضون الحدود الزمنية التي يحددها نظام
حق طلب الحصول على البيانات الشخصية	يحق لأصحاب البيانات الشخصية أن يطلبوا تقديم بياناتهم الشخصية بصيغة منظمة وشائعة الاستخدام وقابلة للقراءة. يجب على شركة سلامة التأكد من تقديم البيانات الشخصية بتنسيق يسمح لصاحب البيانات بإعادة استخدامها أو نقلها إلى جهة تحكم أخرى في البيانات. إذا تم تقديم الطلب بشكل متكرر ويتطلب جهودًا غير عادية بشكل غير معقول من قبل شركة سلامة، فيجوز لشركة سلامة أن تطلب رسومًا معقولة لتزويد أصحاب البيانات بنسخة من بياناتهم الشخصية.
حق طلب تصحيح البيانات الشخصية	يحق لأصحاب البيانات طلب تصحيح البيانات الشخصية غير الدقيقة أو غير المكتملة. يجب أن توفر شركة سلامة عملية مباشرة لأصحاب البيانات لطلب تصحيح بياناتهم الشخصية ويجب أن تضمن اتخاذ إجراءات فورية بشأن هذه الطلبات.
حق طلب إتلاف البيانات الشخصية	يحق لأصحاب البيانات أن يطلبوا إتلاف بياناتهم الشخصية عندما لا تكون ضرورية للأغراض التي جُمعت من أجلها أو إذا سحب صاحب البيانات موافقته. يجب على شركة سلامة ضمان التعامل مع طلبات إتلاف البيانات بشكل آمن، ويجب إبلاغ صاحب البيانات بنتيجة طلبه.

	a reasonable fee for providing the Data Subjects with a copy of their Personal Data.
The Right to Request Correction of Personal Data	Data subjects have the right to request the correction of inaccurate or incomplete Personal Data. SALAMA must provide a straightforward process for data subjects to request the rectification of their Personal Data and must ensure that these requests are acted upon promptly.
The Right to Request Destruction of Personal Data	Data subjects have the right to request the destruction of their Personal Data when it is no longer necessary for the purposes for which it was collected or if the data subject withdraws consent. SALAMA must ensure that data destruction requests are handled securely, and the data subject must be informed of the outcome of their request.
The Right to Withdraw Consent for Personal Data Processing	Data subjects have the right to withdraw their consent for the processing of their Personal Data at any time. SALAMA must follow a process for submitting withdrawal requests, and upon receipt, all processing based on consent must cease immediately.
The Right to Submit Complaints	Data Subjects have the right to submit complaints regarding the processing of their Personal Data. SALAMA must follow clear procedures for handling complaints, and all complaints must be addressed promptly and transparently.

حق سحب الموافقة على معالجة البيانات الشخصية	يحق لأصحاب البيانات سحب موافقتهم على معالجة بياناتهم الشخصية في أي وقت. يجب على شركة سلامة اتباع عملية تقديم طلبات السحب، وعند استلامها، يجب أن تتوقف جميع عمليات المعالجة القائمة على الموافقة على الفور.
حق تقديم الشكاوى	يحق لأصحاب البيانات تقديم شكاوى بشأن معالجة بياناتهم الشخصية. يجب أن توفر شركة سلامة اتباع إجراءات واضحة للتعامل مع الشكاوى، ويجب معالجة جميع الشكاوى بشكل سريع وشفاف.

6. Data Processing Activities

SALAMA engages in a variety of data processing activities, all of which are governed by this policy. To ensure compliance with the KSA PDPL, SALAMA is committed to maintaining detailed records of all Personal Data processing activities.

6.1 Record of Processing Activities (RoPA)

SALAMA maintains a Record of Processing Activities (RoPA) that documents all Personal Data processing activities, including, but not limited to the purposes of processing, categories of data subjects, types of Personal Data, recipients of the data, and any international data transfers.

All departments must contribute to the accuracy and completeness of the RoPA by providing detailed information about their data processing activities including the filled RoPA Template with each processing activity documented into it.

6.2 Privacy Impact Assessment (PIA) and Data Protection Impact Assessments (DPIAs)

Before any new data processing activities, product, system that may pose a high risk to the rights and freedoms of data subjects, SALAMA conducts PIA and as applicable to identify and mitigate any potential risks.

It must be conducted in accordance with KSA PDPL guidelines, and the findings must be documented and reviewed by the Data Privacy Office. Measures must be implemented to mitigate any identified risks before proceeding with the processing activity, product, system.

6.3 Consent Management

Consent is a critical component of the SALAMA's approach to Personal Data processing. SALAMA is committed to ensuring that consent is obtained in a manner that is compliant with the KSA PDPL and that data subjects are fully informed of their rights at the time of consent collection.

6. أنشطة معالجة البيانات

تشارك شركة سلامة في مجموعة متنوعة من أنشطة معالجة البيانات، والتي تخضع جميعها لهذه السياسة. لضمان الامتثال لنظام حماية البيانات الشخصية في المملكة العربية السعودية، تلتزم شركة سلامة بالاحتفاظ بسجلات مفصلة لجميع أنشطة معالجة البيانات الشخصية.

6.1 سجلات أنشطة المعالجة (RoPA)

تحتفظ شركة سلامة بسجل أنشطة المعالجة (RoPA) الذي يوثق جميع أنشطة معالجة البيانات الشخصية، بما في ذلك، على سبيل المثال لا الحصر، أغراض المعالجة، وفئات أصحاب البيانات، وأنواع البيانات الشخصية، ومستلمي البيانات، وأي عمليات نقل دولية للبيانات.

يجب على جميع الإدارات المساهمة في دقة واكتمال سجل أنشطة المعالجة (RoPA) من خلال تقديم معلومات مفصلة حول أنشطة معالجة البيانات الخاصة بهم بما في ذلك نموذج سجل أنشطة المعالجة المعبأ مع توثيق كل نشاط معالجة فيه.

6.2 تقييم أثر الخصوصية (PIA) وتقييم أثر حماية البيانات (DPIA)

قبل أي نشاط لمعالجة البيانات أو منتج أو نظام جديد والذي قد يشكل خطرًا كبيرًا على حقوق وحريات أصحاب البيانات، لابد أن تجري شركة سلامة تقييم أثر الخصوصية وتقييم أثر حماية البيانات حسب الاقتضاء لتحديد أي مخاطر محتملة والتخفيف من حدتها.

يجب إجراء ذلك وفقًا للمبادئ التوجيهية لنظام حماية البيانات في المملكة العربية السعودية، ويجب توثيق النتائج ومراجعتها من قبل مكتب خصوصية البيانات. يجب تنفيذ تدابير للتخفيف من أي مخاطر تم تحديدها قبل الشروع في نشاط المعالجة أو المنتج أو النظام.

6.3 إدارة الموافقة

الموافقة هي عنصر جوهري في نهج سلامة لمعالجة البيانات الشخصية. وتلتزم شركة سلامة بضمان الحصول على الموافقة بطريقة تتوافق مع نظام حماية البيانات الشخصية في المملكة العربية السعودية وأن أصحاب البيانات على علم تام بحقوقهم في وقت جمع تلك الموافقة.

Consent must be freely given, specific, informed, and unambiguous. SALAMA must provide data subjects with clear, accessible information about the purposes of the processing, the legal basis for the processing, and the rights of the data subject. Consent should be obtained before any data processing takes place unless another legal basis for processing applies. SALAMA shall follow a Consent Management Procedure which details the steps related to consent management.

يجب أن تكون الموافقة معطاة بحرية وبشكل محدد ومستنير ولا لبس فيه. يجب أن تزود شركة سلامة أصحاب البيانات بمعلومات واضحة ويمكن الوصول إليها حول أغراض المعالجة والأساس القانوني للمعالجة وحقوق صاحب البيانات. يجب الحصول على الموافقة قبل إجراء أي معالجة للبيانات ما لم ينطبق أساس قانوني آخر للمعالجة. يجب على شركة سلامة اتباع إجراء إدارة الموافقة الذي يفصل الخطوات المتعلقة بإدارة الموافقة.

6.4 Handling Special Categories of Data

6.4 التعامل مع الفئات الخاصة من البيانات

Certain categories of Personal Data, such as sensitive Personal Data, minors' data, and data relating to deceased persons, require special protection under the KSA PDPL.

تتطلب فئات معينة من البيانات الشخصية، مثل البيانات الشخصية الحساسة، وبيانات القُصَّر، والبيانات المتعلقة بالأشخاص المتوفين، حماية خاصة بموجب نظام حماية البيانات الشخصية في المملكة العربية السعودية.

6.4.1 Sensitive Personal Data

6.4.1البيانات الشخصية الحساسة

Sensitive Personal Data includes information related to racial or ethnic origin, religious beliefs, political opinions, health data, genetic data, and biometric data. Processing of such data is subject to stricter requirements.

تشمل البيانات الشخصية الحساسة المعلومات المتعلقة بالأصل العرقي أو الإثني، والمعتقدات الدينية، والآراء السياسية، والبيانات الصحية، والبيانات الجينية، والبيانات البيومترية. تخضع معالجة هذه البيانات لمتطلبات أكثر صرامة.

Sensitive Personal Data may only be processed with the explicit consent of the data subject or under other legal grounds specified by law, such as for health or safety reasons.

لا يجوز معالجة البيانات الشخصية الحساسة إلا بموافقة صريحة من صاحب البيانات أو بموجب أسس قانونية أخرى يحددها النظام، مثل الأسباب الصحية أو أسباب تتعلق بالسلامة.

SALAMA must follow enhanced security measures, including encryption and access controls, when processing sensitive Personal Data.

يجب على شركة سلامة اتباع تدابير أمنية معززة، بما في ذلك التشفير وضوابط الوصول، عند معالجة البيانات الشخصية الحساسة.

Any sharing of sensitive data must be approved by the Data Privacy Office and strictly limited to authorized personnel.

يجب أن تتم الموافقة على أي مشاركة للبيانات الحساسة من قبل مكتب خصوصية البيانات وأن تقتصر بشكل صارم على الأفراد المصرح لهم.

6.4.2 Health Data

6.4.2 البيانات الصحية

Health data is a subset of sensitive Personal Data and must be handled with extreme care, particularly if processed for purposes related to employment, insurance, or medical services.

البيانات الصحية هي مجموعة فرعية من البيانات الشخصية الحساسة ويجب التعامل معها بعناية فائقة، خاصةً إذا تمت معالجتها لأغراض تتعلق بالتوظيف أو التأمين أو الخدمات الطبية.

Health data must only be processed for purposes, such as providing healthcare services, managing health insurance claims, or complying with health and safety regulations.

يجب معالجة البيانات الصحية فقط لأغراض مثل تقديم خدمات الرعاية الصحية أو إدارة مطالبات التأمين الصحي أو الامتثال للوائح الصحة والسلامة.

SALAMA must limit access to health data to authorized personnel and ensure that health data is stored securely.

يجب على شركة سلامة أن تقتصر الوصول إلى البيانات الصحية على الموظفين المصرح لهم وضمان تخزين البيانات الصحية بشكل آمن.

Data subjects must be informed of how their health data will be processed, and explicit consent must be obtained where required by law.

يجب إبلاغ الأشخاص المعنيين بالبيانات بكيفية معالجة بياناتهم الصحية، ويجب الحصول على موافقة صريحة حيثما يقتضي النظام ذلك.

6.4.3 Credit Data

6.4.3 البيانات الائتمانية

Credit data, including bank account details, financial history, credit scores, and policy and claims information, is highly sensitive and must be protected from unauthorized access or misuse.

تعتبر البيانات الائتمانية، بما في ذلك تفاصيل الحساب المصرفي والتاريخ المالي والنتائج الائتمانية ومعلومات البوليصة والمطالبات، حساسة للغاية ويجب حمايتها من الوصول غير المصرح به أو إساءة الاستخدام.

SALAMA shall process Credit Data in a manner that ensures the preservation of the privacy of Data Subjects and protects their rights.

يجب على شركة سلامة معالجة البيانات الائتمانية بطريقة تضمن الحفاظ على خصوصية أصحاب البيانات وحماية حقوقهم.

SALAMA must implement strict access controls and security measures to protect credit data from unauthorized access, including encryption and multi-factor authentication if possible.

يجب أن تطبق شركة سلامة ضوابط وصول صارمة وتدابير أمنية لحماية البيانات الائتمانية من الوصول غير المصرح به، بما في ذلك التشفير والمصادقة المتعددة إن أمكن.

Credit data may only be shared with third parties, such as financial institutions or credit agencies, with the explicit consent of the data subject or as required by law.

لا يجوز مشاركة البيانات الائتمانية مع أطراف ثالثة، مثل المؤسسات المالية أو وكالات الائتمان، إلا بموافقة صريحة من صاحب البيانات أو وفقًا لما يقتضيه النظام.

6.4.4 Handling Personal Data for Vulnerable Individuals and Minors

6.4.4 التعامل مع البيانات الشخصية للأفراد عديمي الأهلية أو القصّر

Personal Data of minors and individuals lacking legal capacity requires additional protection. SALAMA is committed to ensuring that the rights of these individuals are respected and that their data is processed in accordance with the law.

تتطلب البيانات الشخصية للقاصرين والأفراد الذين يفتقرون إلى الأهلية القانونية حماية إضافية. تلتزم شركة سلامة بضمان احترام حقوق هؤلاء الأفراد ومعالجة بياناتهم وفقًا للنظام والقانون.

Consent for processing the Personal Data of minors (those under 18 years of age) must be obtained from a parent or legal guardian.

يجب الحصول على الموافقة على معالجة البيانات الشخصية للقاصرين (الذين تقل أعمارهم عن 18 عامًا) من أحد الوالدين أو الوصي القانوني.

Data subjects lacking legal capacity, such as those under guardianship, must have their data processed with the consent of their guardian or legal representative.

يجب أن تتم معالجة البيانات الخاصة بالأشخاص الذين يفتقرون إلى الأهلية القانونية، مثل الأشخاص الخاضعين للوصاية، بموافقة ولي الأمر أو الممثل القانوني.

Privacy notices aimed at minors must be written in a language and format that is easy to understand.

يجب كتابة إشعارات الخصوصية الموجهة للقُصّر بلغة وصيغة يسهل فهمها.

6.4.5 Deceased Persons' Data

6.4.5 بيانات الأشخاص المتوفين

Deceased persons Personal Data have the same legal rights as living individuals, their Personal Data must be handled with respect and confidentiality, particularly where it may affect the rights of living relatives or beneficiaries.

يحق البيانات الشخصية للأشخاص المتوفين بالحقوق القانونية نفسها التي يتمتع بها الأفراد الأحياء، ويجب التعامل مع بياناتهم الشخصية باحترام وسرية، خاصةً عندما قد تؤثر على حقوق الأقارب الأحياء أو المستفيدين.

Personal Data related to deceased persons must be retained for as long as necessary to fulfill legal or contractual obligations, such as resolving legal claims.

يجب الاحتفاظ بالبيانات الشخصية المتعلقة بالأشخاص المتوفين طالما كان ذلك ضروريًا للوفاء بالالتزامات القانونية أو التعاقدية، مثل تسوية المطالبات القانونية.

Data related to deceased persons must be securely disposed of once it is no longer required, in line with SALAMA's data storage and retention policy.

يجب التخلص من البيانات المتعلقة بالأشخاص المتوفين بشكل آمن بمجرد أن تصبح غير مطلوبة، بما يتماشى مع سياسة تخزين البيانات والاحتفاظ بها لدى شركة سلامة.

SALAMA must ensure that any requests related to the data of deceased persons, such as from legal heirs, are handled in accordance with applicable laws.

يجب على شركة سلامة ضمان التعامل مع أي طلبات تتعلق ببيانات الأشخاص المتوفين، مثل الطلبات المقدمة من الورثة الشرعيين، وفقًا للقوانين المعمول بها.

6.5 Personal Data for Marketing Usage

6.5 الاستخدامات التسويقية للبيانات الشخصية

Personal Data with the exception of sensitive data may be processed for marketing purposes, if it is collected directly from the Data Subjects, and his/her agreement is obtained with applying the PDPL advertising and awareness-raising provisions concerning marketing.

قد تتم معالجة البيانات الشخصية باستثناء البيانات الحساسة لأغراض التسويق، إذا تم جمعها مباشرةً من أصحاب البيانات، وتم الحصول على موافقتهم مع تطبيق أحكام نظام حماية البيانات الشخصية الخاصة بالدعاية والتوعية المتعلقة بالتسويق.

7. Technical and Organizational Measures

7. التدابير التقنية والتنظيمية

7.1 Security Measures

7.1 التدابير الأمنية

SALAMA shall implement a range of security measures to protect Personal Data, including:

تطبق شركة سلامة مجموعة من التدابير الأمنية لحماية البيانات الشخصية، بما في ذلك:

- Access Controls: Access to Personal Data is restricted to authorized personnel only.
- ضوابط الوصول: يقتصر الوصول إلى البيانات الشخصية على الموظفين المصرح لهم فقط. يتم تحديد مستويات الوصول على

Access levels are determined based on the principle of least privilege, ensuring that employees have access to the data necessary for their role, and no more.

أساس مبدأ الحد الأدنى من الامتيازات، مما يضمن وصول الموظفين إلى البيانات اللازمة لدورهم وليس أكثر من ذلك.

- Encryption: Personal Data must be encrypted both in transit and at rest to protect it from unauthorized access.
- التشفير: يجب تشفير البيانات الشخصية أثناء نقلها وعند تخزينها لحمايتها من الوصول غير المصرح به.
- Cybersecurity Controls : Such as firewalls, periodic malware scans and anti-virus protection to reduce the likelihood of personal data leakage and to identify vulnerabilities.
- ضوابط الأمن السيبراني: مثل جدران الحماية والفحص الدوري للبرمجيات الخبيثة والحماية من الفيروسات لتقليل احتمالية تسرب البيانات الشخصية وتحديد نقاط الضعف.
- Data Minimization: Only collecting and retaining the Personal Data necessary for the provision of its services, reducing the risk associated with excessive data storage.
- تقليل البيانات: جمع والاحتفاظ بالبيانات الشخصية الضرورية فقط لتقديم الخدمات اللازمة، مما يقلل من المخاطر المرتبطة بالتخزين المفرط للبيانات.
- Physical Security: Physical access to data centers and storage facilities is strictly controlled, with surveillance systems and access logs maintained at all times.
- الأمن المادي: يخضع الوصول المادي إلى مراكز البيانات ومرافق التخزين لرقابة صارمة، مع الحفاظ على أنظمة المراقبة وسجلات الوصول في جميع الأوقات.
- Incident Response Plan: Devolving incident response plan that outlines the procedure to be followed in the event of a Personal Data breach.
- خطة الاستجابة للحوادث: تطوير خطة الاستجابة للحوادث التي تحدد الإجراءات الواجب اتباعها في حالة حدوث انتهاك للبيانات الشخصية.

All employees, contractors, and third-party processors are required to adhere to the SALAMA's security protocols and report any security incidents or vulnerabilities immediately to the Cyber Security Department and Data Privacy Office.

يُتطلب من جميع الموظفين والمتعاقدين ومعالجي الطرف الثالث الالتزام ببروتوكولات سلامة الأمنية والإبلاغ عن أي حوادث أو ثغرات أمنية على الفور إلى إدارة الأمن السيبراني ومكتب خصوصية البيانات.

7.2 Privacy by Design and Default

7.2الخصوصية حسب التصميم والإفتراض

SALAMA shall implement technical and organizational measures, from the start at the earliest stages of the design of the processing operations, to safeguard privacy and Personal Data Protection principles and ensure the protection of Data Subjects rights as per the SALAMA's privacy by design policy.

يجب على شركة سلامة تنفيذ تدابير تقنية وتنظيمية، منذ البداية في المراحل الأولى من تصميم عمليات المعالجة، لحماية الخصوصية ومبادئ حماية البيانات الشخصية وضمان حماية حقوق أصحاب البيانات وفقًا لسياسة الخصوصية حسب التصميم الخاصة بشركة سلامة.

- Salama shall adopt a Privacy by Design and Default approach, taking privacy requirements into account throughout the lifecycle of systems and processes. This includes:
- يجب على سلامة اعتماد نهج الخصوصية حسب التصميم والافتراض، مع مراعاة متطلبات الخصوصية طوال دورة حياة الأنظمة والعمليات. ويشمل ذلك:

- Considering Data Privacy at the requirements and design stages of any new process, system, or data collection.
- Integrating appropriate technical and organizational measures to protect Personal Data, such as pseudonymization, encryption, access controls, etc.
- Ensuring privacy settings are set to maximum by default and that only data necessary for each specific purpose is collected.
- Conducting Data Protection Impact Assessments for high-risk processing activities.
- Documenting measures taken to demonstrate compliance.
- SALAMA shall always ensure that Personal Data is processed with the highest privacy protection, so that by default Personal Data is only accessible to concerned individuals. SALAMA shall implement required mechanisms for ensuring that, by default, only those Personal Data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes.
- Prior to engaging in new activities or implementing, updating, or purchasing new technologies, SALAMA shall consider the impact and risks these actions may have on the privacy of the Data Subject through performing risk assessments and conducting a Data Privacy Impact Assessment (DPIA), where required.
- SALAMA shall prioritize privacy-friendly technical or organizational solutions whenever possible, considering the specific risks for the Data Subjects' rights, freedoms, and safety, while balancing the technological possibilities with the financial costs.

- مراعاة خصوصية البيانات في متطلبات ومراحل تصميم أي عملية أو نظام أو عند جمع بيانات جديدة.
- إدماج التدابير التقنية والتنظيمية المناسبة لحماية البيانات الشخصية، مثل الترميز، والتشفير، وضوابط الوصول، وما إلى ذلك.
- التأكد من ضبط إعدادات الخصوصية على الحد الأقصى افتراضيًا وأن البيانات الضرورية فقط لكل غرض محدد يتم جمعها.
- إجراء تقييمات تأثير حماية البيانات لأنشطة المعالجة عالية المخاطر.
- توثيق التدابير المتخذة لإثبات الامتثال.
- يجب على شركة سلامة أن تضمن دائمًا معالجة البيانات الشخصية بأعلى درجات حماية الخصوصية، بحيث لا يمكن الوصول إلى البيانات الشخصية افتراضيًا إلا للأفراد المعنيين. يجب على شركة سلامة تنفيذ الآليات المطلوبة لضمان أن تتم معالجة البيانات الشخصية بشكل افتراضي فقط تلك البيانات الشخصية الضرورية لكل غرض محدد من أغراض المعالجة ولا يتم جمعها أو الاحتفاظ بها بشكل خاص بما يتجاوز الحد الأدنى الضروري لتلك الأغراض.
- قبل الانخراط في أنشطة جديدة أو تنفيذ أو تحديث أو شراء تقنيات جديدة، يجب على شركة سلامة النظر في التأثير والمخاطر التي قد تنطوي عليها هذه الإجراءات على خصوصية صاحب البيانات من خلال إجراء تقييمات للمخاطر وإجراء تقييم تأثير خصوصية البيانات (DPIA)، عند الاقتضاء.
- يجب على شركة سلامة إعطاء الأولوية للتقنيات التي تراعي الخصوصية
- يجب على شركة سلامة إعطاء الأولوية للحلول التقنية أو التنظيمية الملائمة للخصوصية كلما كان ذلك ممكنًا، مراعاة للمخاطر المحددة على حقوق أصحاب البيانات وحرياتهم وسلامتهم، مع الموازنة بين الإمكانيات التكنولوجية والتكاليف المالية.

7.3 Email and Document Management

SALAMA shall manage all emails and documents containing Personal Data in a way that ensures compliance with the rules outlined in this policy, particularly to avoid using multiple copies of documents containing Personal Data, and the safe storage and/or destruction of documents. SALAMA retains the discretion to adopt additional rules as necessary.

- To ensure the documents and emails are classified as per Data Classification Policy.
- To ensure security of Personal Data contained in emails and documents, SALAMA shall:
  Use secure email protocols and encryption for external emails containing Personal Data.
- Include confidentiality notices in emails.
- Manage document access permissions based on job roles.
- Store Personal Data only in secure locations with backup.
- Dispose of documents containing Personal Data securely, e.g., using shredders.

7.3 إدارة البريد الإلكتروني والوثائق

يجب على شركة سلامة إدارة جميع رسائل البريد الإلكتروني والمستندات التي تحتوي على بيانات شخصية بطريقة تضمن الامتثال للقواعد الموضحة في هذه السياسة، ولا سيما لتجنب استخدام نسخ متعددة من المستندات التي تحتوي على بيانات شخصية، والتخزين الآمن و/أو إتلاف المستندات. تحتفظ شركة سلامة بالسلطة التقديرية لاعتماد قواعد إضافية حسب الضرورة.

- ضمان تصنيف المستندات ورسائل البريد الإلكتروني وفقًا لسياسة تصنيف البيانات.
- ضماناً لأمن البيانات الشخصية الواردة في رسائل البريد الإلكتروني والوثائق، يجب على شركة سلامة استخدام بروتوكولات البريد الإلكتروني الآمنة والتشفير لرسائل البريد الإلكتروني الخارجية التي تحتوي على بيانات شخصية.
- تضمين إشعارات السرية في رسائل البريد الإلكتروني.
- إدارة أذونات الوصول إلى المستندات بناءً على الأدوار الوظيفية.
- تخزين البيانات الشخصية في مواقع آمنة فقط مع النسخ الاحتياطي.
- التخلص من المستندات التي تحتوي على بيانات شخصية بشكل آمن، على سبيل المثال، باستخدام آلات تمزيق الورق.

7.4 Restriction on Copying of Official Documents

All official data is the property of SALAMA and unauthorized copying, or distribution is prohibited. Data may only be used for the purposes outlined in the privacy policy and that copying for other purposes is not allowed.

- SALAMA shall clearly outline the consequences for unauthorized copying, including disciplinary actions, legal repercussions, and potential termination of employment or contracts.
- SALAMA shall establish and follow monitoring mechanisms to track access and copying of data. Regular audits should be conducted to ensure compliance with data usage policies.

7.4. القيود المفروضة على نسخ الوثائق الرسمية

جميع البيانات الرسمية هي ملك لشركة سلامة ويحظر النسخ أو التوزيع غير المصرح به. لا يجوز استخدام البيانات إلا للأغراض المبينة في سياسة الخصوصية ولا يُسمح بالنسخ لأغراض أخرى.

- يجب على شركة سلامة أن تحدد بوضوح عواقب النسخ غير المصرح به، بما في ذلك الإجراءات التأديبية والتداعيات القانونية واحتمال إنهاء التوظيف أو العقود.
- يجب على شركة سلامة إنشاء واتباع آليات مراقبة لتتبع الوصول إلى البيانات ونسخها. يجب إجراء عمليات تدقيق منتظمة لضمان الامتثال لسياسات استخدام البيانات.

8. Data Sharing and Disclosure

Data sharing and disclosure is a part of day-to-day business process requirements. SALAMA must share or disclose personal data in accordance with applicable laws and regulations and as per SALAMA Data Sharing Policy and Data Privacy Guidelines.

8. مشاركة وإفصاح البيانات

تعد مشاركة البيانات والإفصاح عنها جزءًا من متطلبات العمليات التجارية اليومية. يجب على شركة سلامة مشاركة البيانات الشخصية أو الإفصاح عنها وفقًا للأنظمة والقوانين المعمول بها ووفقًا لسياسة مشاركة البيانات وإرشادات خصوصية البيانات الخاصة بشركة سلامة.

9. Data Retention, Disposal, and Transfer of Personal Data

9. الاحتفاظ بالبيانات والتخلص منها ونقلها

9.1 Retention Periods

Personal Data will only be retained for as long as necessary to fulfill the purposes for which it was collected, or as required by applicable laws and regulations. SALAMA shall establish retention periods for various types of Personal Data, which are documented in a Data Storage and Retention Policy.

- Each department is responsible for ensuring that Personal Data is retained in line with the Salama's Data Storage and Retention Policy.
- The retention schedule must be reviewed annually by the Data Privacy Office to ensure compliance with any changes in legal, regulatory, or business requirements.
- SALAMA will notify data subjects of the retention periods for their Personal Data as required by law, typically in privacy notices or at the point of data collection.

9.1 فترات الاحتفاظ

سيتم الاحتفاظ بالبيانات الشخصية فقط طالما كان ذلك ضروريًا للوفاء بالأغراض التي تم جمعها من أجلها، أو وفقًا لما تقتضيه الأنظمة واللوائح المعمول بها. تحدد شركة سلامة فترات الاحتفاظ بأنواع مختلفة من البيانات الشخصية، والتي يتم توثيقها في سياسة تخزين البيانات والاحتفاظ بها.

- كل قسم مسؤول عن ضمان الاحتفاظ بالبيانات الشخصية بما يتماشى مع سياسة سلامة لتخزين البيانات والاحتفاظ بها.
- يجب مراجعة جدول الاحتفاظ بالبيانات سنوياً من قبل مكتب خصوصية البيانات لضمان الامتثال لأي تغييرات في المتطلبات القانونية أو التنظيمية أو التجارية.
- ستقوم شركة سلامة بإخطار أصحاب البيانات بفترات الاحتفاظ ببياناتهم الشخصية وفقًا لما يقتضيه النظام، وعادةً ما يكون ذلك في إشعارات الخصوصية أو عند جمع البيانات.

9.2 Secure Disposal of Personal Data

Once the retention period for Personal Data has expired, or when Personal Data is no longer required for the purpose for which it was collected, SALAMA shall securely dispose of the data as per Secure Disposal Standard and Personal Data Destruction guidelines (Data Privacy Guidelines) in a manner that ensures it cannot be recovered or misused.

- Paper-based records containing Personal Data must be shredded, incinerated, or

9.2 التخلص الآمن من البيانات الشخصية

بمجرد انتهاء فترة الاحتفاظ بالبيانات الشخصية، أو عندما لا تعود البيانات الشخصية مطلوبة للغرض الذي جُمعت من أجله، تتخلص شركة سلامة من البيانات بشكل آمن وفقًا لمعايير التخلص الآمن وإرشادات إتلاف البيانات الشخصية (إرشادات خصوصية البيانات) بطريقة تضمن عدم إمكانية استعادتها أو إساءة استخدامها.

- يجب تمزيق السجلات الورقية التي تحتوي على بيانات شخصية أو حرقها أو التخلص منها بشكل آمن من خلال خدمة معتمدة من طرف ثالث للتخلص منها.

disposed of securely through a certified third-party disposal service.

- Electronic data must be securely erased using appropriate data destruction software or physical destruction techniques to ensure it cannot be recovered.
- Backup data must also be securely deleted, and any remaining Personal Data must be anonymized or pseudonymized where necessary for archival purposes.

- يجب محو البيانات الإلكترونية بشكل آمن باستخدام برامج تدمير البيانات المناسبة أو تقنيات التدمير المادي لضمان عدم إمكانية استعادتها.
- يجب أيضًا حذف بيانات النسخ الاحتياطية بشكل آمن، ويجب أن تكون أي بيانات شخصية متبقية مجهولة الهوية أو بأسماء مستعارة (الترميز) عند الضرورة لأغراض الأرشفة.

9.3 Data Transfers Within KSA

9.3 نقل البيانات داخل المملكة العربية السعودية

SALAMA shall only transfer Personal Data within the Kingdom of Saudi Arabia when it is necessary to fulfill the purposes for which the data was originally collected, or for legitimate business operations. All internal transfers must adhere to strict data protection standards.

يجب على شركة سلامة نقل البيانات الشخصية داخل المملكة العربية السعودية فقط عندما يكون ذلك ضروريًا للوفاء بالأغراض التي تم جمع البيانات من أجلها في الأصل، أو للعمليات التجارية المشروعة. يجب أن تلتزم جميع عمليات النقل الداخلي بمعايير صارمة لحماية البيانات.

- Transfers of Personal Data between departments or subsidiaries within KSA must be logged, and access controls must be applied to ensure that only authorized personnel can access the data.
- Data transfer agreements must be in place between entities to safeguard the Personal Data being shared.

- يجب تسجيل عمليات نقل البيانات الشخصية بين الإدارات أو الشركات التابعة داخل المملكة العربية السعودية، ويجب تطبيق ضوابط الوصول لضمان أن الموظفين المصرح لهم فقط هم من يمكنهم الوصول إلى البيانات.
- يجب تطبيق اتفاقيات نقل البيانات بين الجهات لحماية البيانات الشخصية التي تتم مشاركتها.

9.4 Data Transfers Outside KSA

9.4 نقل البيانات خارج المملكة العربية السعودية

SALAMA shall only transfer Personal Data outside of KSA if one of the following conditions is met:

- The destination country ensures an adequate level of data protection as determined by the Competent Authority.
- The transfer is necessary for the performance of a contract or at the request of the data subject.
- Appropriate safeguards are in place, such as binding corporate rules or standard contractual clauses.
- The Legal Department, in collaboration with the Data Privacy Office, must review and approve all international data transfers.

لا يجوز لشركة سلامة نقل البيانات الشخصية خارج المملكة العربية السعودية إلا في حالة استيفاء أحد الشروط التالية

- أن يضمن بلد الوجهة مستوى كافٍ من حماية البيانات على النحو الذي تحدده السلطة المختصة.
- النقل ضروري لتنفيذ عقد أو بناء على طلب صاحب البيانات.
- وجود ضمانات مناسبة، مثل القواعد المؤسسية الملزمة أو البنود التعاقدية القياسية.
- يجب على الإدارة القانونية، بالتعاون مع مكتب خصوصية البيانات، مراجعة جميع عمليات نقل البيانات الدولية والموافقة عليها.
- قبل إجراء أي عملية نقل، يجب إجراء تقييم لمخاطر خصوصية/حماية البيانات وغيرها من التقييمات لضمان توفير الحماية الكافية للبيانات الشخصية في بلد الوجهة.

- Before any transfer, a Data privacy/protection risk assessment and other assessments must be conducted to ensure that adequate protection for Personal Data is provided in the destination country.
- Where required, the data subject must be informed, and their explicit consent obtained before their Personal Data is transferred outside of KSA.

9.5 Third-Party Vendor Management

SALAMA works with third-party vendors, suppliers, and service providers who may process Personal Data on its behalf. It is critical that all third-party vendors comply with the SALAMA's data protection standards and KSA PDPL requirements.

9.5.1 Vendor Due Diligence and Contracts

Before engaging a third-party vendor that will process Personal Data, SALAMA must conduct due diligence such third party data protection risk assessment to ensure that the vendor has appropriate data protection measures in place. A legally binding contract covering personal data protection law requirements must be in place with every vendor that processes Personal Data on behalf of the SALAMA.

The Legal Department must ensure that all third-party vendors sign a contract covering personal data protection law requirements before any Personal Data is shared. The contract must outline the roles and responsibilities of the vendor and the SALAMA, as well as the security measures the vendor must implement to protect the Personal Data.

The SALAMA will conduct regular audits and assessments of third-party vendors to verify compliance with data protection requirements.

- عند الاقتضاء، يجب إبلاغ صاحب البيانات والحصول على موافقته الصريحة قبل نقل بياناته الشخصية خارج المملكة العربية السعودية.

9.5 إدارة الموردين والأطراف الثالثة

تعمل شركة سلامة مع الموردين ومقدمي الخدمات من الأطراف الثالثة الذين قد يعالجون البيانات الشخصية نيابة عنها. يُعد من الضروري أن يمتثل جميع الموردين وجهات الأطراف الثالثة المتعاقد معها لمعايير حماية البيانات الخاصة بشركة سلامة ومتطلبات نظام حماية البيانات الشخصية في المملكة العربية السعودية.

9.5.1 إجراءات التحقق اللازمة للموردين/ الأطراف الثالثة وعقودهم

قبل التعاقد مع أي مورد أو طرف ثالث لمعالجة البيانات الشخصية، يجب على شركة سلامة إجراء التحقق اللازم مثل تقييم مخاطر حماية البيانات للأطراف الثالثة للتأكد من أن المورد لديه تدابير مناسبة لحماية البيانات. يجب أن يكون هناك عقد ملزم قانونيًا يغطي متطلبات نظام حماية البيانات الشخصية مع كل طرف ثالث يقوم بمعالجة البيانات الشخصية نيابةً عن شركة سلامة.

يجب على الإدارة القانونية التأكد من توقيع جميع الموردين أو الأطراف الثالثة على عقد يغطي متطلبات نظام حماية البيانات الشخصية قبل مشاركة أي بيانات شخصية. يجب أن يحدد العقد أدوار ومسؤوليات المورد وشركة سلامة، بالإضافة إلى التدابير الأمنية التي يجب على المورد تنفيذها لحماية البيانات الشخصية.

ستجري شركة سلامة عمليات تدقيق وتقييم منتظمة لموردي الطرف الثالث للتحقق من الامتثال لمتطلبات حماية البيانات.

9.5.2 Third-Party Vendor Audits

SALAMA shall periodically audit third-party vendors to ensure they adhere to the data protection standards outlined in the contract. If any vendor fails to comply, corrective measures must be taken immediately, and the vendor relationship may be terminated.

Vendors must provide evidence of compliance with data protection policies, including security certifications and audit reports.

The Data Privacy Office, in collaboration with the IT Department, must schedule and conduct regular audits of third-party processors.

If a vendor is found to be non-compliant, they must implement corrective actions within a specified time limit.

9.5.2 عمليات تدقيق الموردين والأطراف الثالثة

يجب على شركة سلامة التدقيق بشكل دوري على الموردين الخارجيين للتأكد من التزامهم بمعايير حماية البيانات الموضحة في العقد. وفي حال عدم امتثال أي مورد، يجب اتخاذ التدابير التصحيحية على الفور، ويجوز إنهاء التعاقد مع المورد.

يجب على الموردين تقديم دليل على الامتثال لسياسات حماية البيانات، بما في ذلك شهادات الأمان وتقارير التدقيق.

يجب أن يقوم مكتب خصوصية البيانات، بالتعاون مع إدارة تقنية المعلومات، بجدولة وإجراء عمليات تدقيق منتظمة لمعالجات الطرف الثالث.

وعند تبين أن المورد غير ممتثل، فيجب عليه تنفيذ إجراءات تصحيحية في غضون مهلة زمنية محددة.

10. Personal Data Breach

SALAMA endeavors to protect Personal Data to the best of its abilities. Despite its best efforts, technical or organizational security could be breached by accident or intentionally, and this may result in the confidentiality, integrity, or availability of Personal Data being compromised. SALAMA shall follow a Personal Data Breach Management Procedure which details the response process in case of Personal Data breaches.

10. تسرب البيانات الشخصية

تسعى شركة سلامة إلى حماية البيانات الشخصية بأفضل ما لديها من الإمكانيات. على الرغم من بذل قصارى جهدها، يمكن أن يتم اختراق الأمن التقني أو التنظيمي عن طريق الخطأ أو بشكل متعمد، وقد يؤدي ذلك إلى انتهاك سرية البيانات الشخصية أو سلامتها أو توافرها. تتبع شركة سلامة إجراءات إدارة انتهاك البيانات الشخصية التي توضح بالتفصيل عملية الاستجابة في حالة حدوث أي انتهاكات للبيانات الشخصية.

11. Automated Decision-Making and Profiling

SALAMA may use automated decision-making and profiling technologies in its operations. These processes involve the use of algorithms to make decisions based on Personal Data without human intervention. Such processes are regulated under KSA PDPL, and SALAMA is committed to ensuring transparency and fairness in their use.

11. اتخاذ القرارات الآلية والتوصيف الآلي

قد تستخدم شركة سلامة تقنيات أتمتة اتخاذ القرارات والتوصيف الآلي في عملياتها. تتضمن هذه العمليات استخدام الخوارزميات لاتخاذ القرارات بناءً على البيانات الشخصية دون تدخل بشري. يتم تنظيم مثل هذه العمليات بموجب نظام حماية البيانات الشخصية في المملكة العربية السعودية، وتلتزم شركة سلامة بضمان الشفافية والإنصاف في استخدامها.

11.1 Use of Automated Decision-Making

Automated decision-making is used by the SALAMA in certain business processes, such as creditworthiness assessments, personalized marketing. Data subjects must be informed if their data will be subject to

11.1 استخدام اتخاذ القرارات الآلية

تُستخدم عملية اتخاذ القرارات الآلية من قبل شركة سلامة في بعض العمليات التجارية، مثل تقييمات الجدارة الائتمانية والتسويق المخصص. يجب إبلاغ أصحاب البيانات إذا كانت بياناتهم ستخضع للمعالجة الآلية ما لم تكن هناك

automated processing unless there is legitimate interest such as fraud detection etc, and they must be given the right to opt-out or request human intervention.

- Automated decision-making processes must be designed and reviewed to ensure they do not negatively impact the rights of data subjects.
- Data subjects must be notified before any automated decisions are made that significantly affect them, and they must be given the option to request human review of the decision.
- SALAMA must implement safeguards to ensure that any biases or inaccuracies in the automated systems are minimized.

مصلحة مشروعة مثل الكشف عن الاحتيال وما إلى ذلك، ويجب منحهم الحق في سحب الموافقة أو طلب التدخل البشري في معالجة بياناتهم.

- يجب تصميم عمليات اتخاذ القرارات المؤتمتة ومراجعتها لضمان عدم تأثيرها السلبي على حقوق أصحاب البيانات.
- يجب إخطار أصحاب البيانات قبل اتخاذ أي قرارات مؤتمتة تؤثر عليهم بشكل كبير، ويجب أن يُتاح لهم خيار طلب مراجعة بشرية لاتخاذ القرار.
- يجب على شركة سلامة تنفيذ ضمانات لضمان تقليل أي تحيزات أو أخطاء في الأنظمة الآلية.

11.2 Profiling and Its Use

Profiling refers to the automated processing of Personal Data to evaluate certain personal characteristics of an individual, such as behavior, preferences, or performance. SALAMA may engage in profiling for marketing purposes, risk assessments, or customer segmentation.

- Profiling activities must be transparent, and data subjects must be provided with information about the logic involved in profiling and its potential consequences.
- SALAMA must ensure that profiling is only conducted where necessary and with appropriate safeguards in place to protect the data subject's rights.
- Data subjects must be able to opt-out of profiling activities related to direct marketing.

11.2 الفحص واستخدامه

يشير الفحص إلى المعالجة الآلية للبيانات الشخصية لتقييم خصائص شخصية معينة للفرد، مثل السلوك أو التفضيلات أو الأداء. قد تشارك شركة سلامة في عملية التوصيف لأغراض التسويق أو تقييم المخاطر أو تجزئة العملاء.

- يجب أن تكون أنشطة الفحص شفافة، ويجب تزويد أصحاب البيانات بمعلومات حول الأسلوب المنطقي الذي ينطوي عليه الفحص وتبعاته المحتملة.
- يجب أن تضمن شركة سلامة ألا يتم إجراء الفحص إلا عند الضرورة ومع وجود ضمانات مناسبة لحماية حقوق صاحب البيانات.
- يجب أن يكون أصحاب البيانات قادرين على إلغاء الموافقة على أنشطة الفحص المتعلقة بالتسويق المباشر.

12. Exceptions and Approval

Any exceptions to this policy should be approved by the Data Privacy Officer as first level of approval, in consultation with the Compliance department and other relevant stakeholders. Final approvals to any amendments to the Privacy policies will be given by the Governance.

12. الاستثناءات والموافقة

يجب أن تتم الموافقة على أي استثناءات من هذه السياسة من قبل مسؤول خصوصية البيانات كمستوى أول من الموافقة، بالتشاور مع قسم الامتثال وأصحاب المصلحة الآخرين ذوي الصلة. سيتم منح الموافقات النهائية على أي تعديلات على سياسات الخصوصية من قبل الحوكمة.

13. Monitoring of Legal / Regulatory Developments

Compliance department will be responsible to communicate any updates in the existing Data Privacy legal / regulatory requirements to all the respective staff members in coordination with Data Privacy Officer. The Data Privacy Office, in coordination with the Legal Department, shall monitor relevant laws, regulations, court decisions and guidance from data protection authorities to identify required changes to this policy. The policy shall be updated as needed to maintain compliance.

13. مراقبة التطورات التشريعية/التنظيمية

سيكون قسم الامتثال مسؤولاً عن إبلاغ أي تحديثات في المتطلبات التشريعية/التنظيمية الحالية لخصوصية البيانات إلى جميع الموظفين المعنيين بالتنسيق مع مسؤول خصوصية البيانات. يجب أن يقوم مكتب خصوصية البيانات، بالتنسيق مع إدارة الشؤون القانونية، بمراقبة الأنظمة واللوائح وقرارات المحاكم والتوجيهات ذات الصلة من سلطات حماية البيانات لتحديد التغييرات المطلوبة في هذه السياسة. يجب تحديث السياسة حسب الحاجة للحفاظ على الامتثال.

14. Internal Audit

An internal audit shall be conducted periodically be SALAMA Internal Audit Department along with Data Privacy Officer. Internal audit shall report the results of this audit to Business Data Owners, Data Governance, Audit Committee, and any other respective stakeholder.

The Internal Audit Department shall periodically review compliance with this policy and report findings to senior management. Audits may include:

- Review of privacy policies, procedures, and documentation
- Evaluation of privacy controls and security measures
- Compliance checks for Data Subject rights, breach notification, international transfers, etc.
- Review of training and awareness programs

Any gaps identified shall be remediated under the oversight of the Data Privacy Officer.

14. المراجعة الداخلية

يجب إجراء مراجعة داخلية بشكل دوري من قبل إدارة المراجعة الداخلية في سلامة مع مسؤول خصوصية البيانات. يجب على المراجعة الداخلية إبلاغ نتائج المراجعة إلى مُلّاك بيانات الأعمال وحوكمة البيانات ولجنة المراجعة وأي جهة معنية أخرى .

يجب على إدارة المراجعة الداخلية مراجعة الامتثال لهذه السياسة بشكل دوري وإبلاغ الإدارة العليا بالنتائج. قد تشمل عمليات التدقيق ما يلي:

- مراجعة سياسات الخصوصية وإجراءاتها ووثائقها
- تقييم ضوابط الخصوصية والتدابير الأمنية
- التحقق من الامتثال لحقوق أصحاب البيانات، والإخطار بالانتهاكات، وعمليات النقل الدولية، وما إلى ذلك.
- مراجعة برامج التدريب والتوعية

يجب معالجة أي ثغرات يتم تحديدها تحت إشراف مسؤول خصوصية البيانات.

15. Review and Evaluation

The SALAMA Privacy Policy shall be reviewed at the time of any major change(s) in the existing environment affecting privacy policies and procedures or every year, whichever is earlier. This document shall be reviewed by the privacy office in consultation with

15. المراجعة والتقييم

يجب مراجعة سياسة الخصوصية الخاصة بشركة سلامة في وقت حدوث أي تغيير (تغييرات) رئيسية في البيئة الحالية التي تؤثر على سياسات وإجراءات الخصوصية أو كل عام، أيهما أسبق. يجب أن تتم مراجعة هذه الوثيقة من قبل مكتب الخصوصية بالتشاور مع مختصي الخصوصية وسيتم اعتمادها من قبل مكتب خصوصية البيانات.

privacy champions and will be approved by the Data Privacy Office.

The review process shall involve:

- Evaluation of the effectiveness of current policy requirements
- Analysis of privacy KPIs and audit findings
- Incorporation of new best practices
- Stakeholder consultation

يجب أن تتضمن عملية المراجعة:

- تقييم فعالية متطلبات السياسة الحالية
- تحليل مؤشرات الأداء الرئيسية للخصوصية ونتائج التدقيق
- دمج أفضل الممارسات الجديدة
- التشاور مع أصحاب المصلحة