سياسة حماية البيانات

تحكم هذه السياسة كيفية قيام شركة "سوبيريور إنرجي سيرفيسز" (Superior Energy Services) (يُشار إليها باسم "**سوبيريور**" أو "**الشركة**" أو "**نحن**" أو "**هم**") بجمع المعلومات الشخصية الموجودة في حوزتها واستخدامها وتخزينها واستبقائها ومشاركتها وحمايتها. قد تتعلق هذه المعلومات الشخصية بموظفي الشركة السابقين أو الحاليين أو المرشحين المحتملين.

يتعين على جميع موظفي الشركة قراءة هذه السياسة وفهمها والالتزام ببنودها عند المشاركة في جمع المعلومات الشخصية و/أو معالجتها في سياق عملهم. يُرجى التواصل مع مكتب حماية البيانات عبر البريد الإلكتروني dataprotection@superiorenergy.com في حال وجود أي استفسارات عن آليات تشغيل هذه السياسة، أو إذا كانت لديكم أي مخاوف بشأن عدم الالتزام بها أو وجود مخالفات في اتباعها.

تحتفظ الشركة بالحق في تعديل هذه السياسة في أي وقت، وستكون النسخة الأحدث متاحة دائمًا على الشبكة الداخلية (Intranet) الخاصة بالشركة.

1- أنواع المعلومات الشخصية وأنشطة المعالجة

يُقصد بمصطلح "**المعلومات الشخصية**" في هذه السياسة أي معلومات تتعلق بفرد محدد أو فرد يمكن تحديده، ويشمل ذلك على سبيل المثال لا الحصر: الاسم وتاريخ الميلاد ومعلومات الاتصال والمعرفات الحكومية والبيانات الديموغرافية والبيانات المالية والبيانات الطبية والبيانات المهنية والبيانات التعليمية والاستنتاجات المستخلصة بشأن الفرد، وغيرها. تُعد "**المعلومات الشخصية الحساسة**" فئة فرعية من المعلومات الشخصية التي تتطلب عناية فائقة في التعامل معها، مثل: العِرق والدين والتوجه الجنسي والبيانات الطبية والمقاييس البيومترية والموقع الجغرافي والمعرفات الحكومية.

على موظفي الشركة الرجوع إلى "إشعار خصوصية الموقع الإلكتروني" و"إشعار خصوصية الموظف" المتاحين على الشبكة الداخلية للشركة للحصول على وصف شامل لأنواع المعلومات الشخصية، بما في ذلك المعلومات الشخصية الحساسة التي تقوم الشركة بجمعها ومعالجتها لمختلف فئات الأفراد (مثل الموظفين والمقاولين وزوار الموقع الإلكتروني والعملاء الحاليين والمحتملين، وغيرهم من الأفراد الذين يتفاعلون مع الشركة). يرجى تذكر أنه يمكن تحديد هوية الفرد بشكل مباشر من خلال البيانات وحدها، أو بشكل غير مباشر من خلال ربط البيانات بعوامل أو معرفات أخرى. يُشار إلى الشخص المُحددة هويته باسم "**صاحب البيانات**".

وتشمل "**المعالجة**" جمع المعلومات الشخصية، أو تسجيلها، أو استخدامها، أو الاحتفاظ بها، أو إجراء أي عملية أو مجموعة عمليات عليها، بما في ذلك تنظيمها أو تعديلها أو استرجاعها أو الإفصاح عنها أو نقلها أو مسحها أو إتلافها.

2- مبادئ حماية البيانات

تلتزم الشركة بمبادئ حماية البيانات التالية، ونتوقع من جميع الموظفين الالتزام بها عند معالجة المعلومات الشخصية نيابةً عن الشركة:

القانونية والعدالة والشفافية يجب معالجة المعلومات الشخصية بطريقة قانونية وعادلة وشفافة. تخضع أي عملية معالجة للمعلومات الشخصية نقوم بها لواحد أو أكثر من الأسس القانونية التالية:

أ) تقديم صاحب البيانات موافقته على المعالجة.
ب) ضرورة المعالجة لتنفيذ العقد مع صاحب البيانات.

ج) ضرورة المعالجة للوفاء بالتزاماتنا بالامتثال القانوني.
د) ضرورة المعالجة لحماية المصالح الحيوية لصاحب البيانات؛ و/أو
هـ) ضرورة عملية المعالجة سعيًا وراء مصالحنا المشروعة أو مصالح طرف ثالث، شريطة ألا تطغى مصالحُ صاحب البيانات أو حقوقه وحرياته الأساسية على هذه المصالح المشروعة.

يتم توفير المعلومات المتعلقة بكيفية وسبب جمعنا للمعلومات الشخصية، والأسس القانونية التي نعتمد عليها، لجميع أصحاب البيانات في "إشعار خصوصية الموقع الإلكتروني" و"إشعار خصوصية الموظف".

تحديد الغرض. يجب جمع المعلومات الشخصية لأغراض محددة وصريحة ومشروعة، ولا يجوز معالجتها لاحقًا بطريقة تتعارض مع تلك الأغراض. يتم الإفصاح عن أغراض الجمع لصاحب البيانات في "إشعار خصوصية الموقع الإلكتروني" أو "إشعار خصوصية الموظف"، وسنقوم بإبلاغ صاحب البيانات قبل معالجة معلوماته الشخصية لأي غرض لم يتم الإفصاح عنه مسبقًا.

الحد من البيانات. يجب أن تكون المعلومات الشخصية التي يتم جمعها ملائمة وذات صلة ومقتصرة فقط على القدر والأنواع الضرورية لتحقيق الغرض (أو الأغراض) المعلن عنها للجمع. علاوة على ذلك، لا يجوز الاحتفاظ بالمعلومات الشخصية إلا للفترة الضرورية لتحقيق الغرض (أو الأغراض) المعلن عنها للجمع. تأخذ الشركة في اعتبارها المتطلبات القانونية أو المحاسبية أو التقارير الرقابية، مثل قوانين التقادم المعمول بها، والتحقيقات التنظيمية و/أو التقاضي، عند تحديد مدة الاحتفاظ بالمعلومات الشخصية.

الدقة. يجب أن تكون المعلومات الشخصية دقيقة، وسنتخذ جميع الخطوات المعقولة لإتلاف أو تعديل المعلومات الشخصية غير الدقيقة أو القديمة.

النزاهة والسرية. نحن نضع تدابير أمنية مادية وتقنية وتنظيمية مناسبة لمنع التدمير العرضي أو غير القانوني للمعلومات الشخصية التي في عهدة الشركة أو فقدانها أو سرقتها أو تغييرها أو الإفصاح عنها أو الوصول إليها دون تصريح ("اختراق البيانات"). على موظفي الشركة المشاركين في معالجة المعلومات الشخصية، سواء كانوا يعملون في مقر الشركة، أو عن بُعد، أو من المنزل، أو في مواقع العملاء، بما في ذلك عند معالجة المعلومات الشخصية على الأجهزة الشخصية، اتباع جميع الإجراءات والضمانات التقنية المعمول بها للحفاظ على الأمن بدءًا من مرحلة الجمع وصولاً إلى مرحلة الإتلاف. يمكن إيجاد على مزيد من المعلومات في القسم 3 من هذه السياسة، وفي سياسة تكنولوجيا المعلومات الخاصة بنا، وخطة الاستجابة للحوادث الكبرى، وخطة استعادة تكنولوجيا المعلومات للمؤسسات في حالات الكوارث، والتي يمكن الوصول إليها جميعًا عبر شبكة الشركة الداخلية (Intranet).

المساءلة. تعد الشركة مسؤولة عن الامتثال لمبادئ حماية البيانات بموجب القانون المعمول به، ويجب أن يمكنها إثبات ذلك. إن سياساتنا وإجراءاتنا وإشعاراتنا، بالإضافة إلى أي إرشادات وتدريبات وسجلات وعمليات تدقيق داخلي، تعد دليلاً على التزامنا بحماية البيانات وبمبدأ المساءلة.

3- الخطوات التي نتخذها لتحديد مخاطر الخصوصية والحد منها

تقييمات أثر حماية البيانات (DPIA)

في ظل ظروف معينة قد تؤثر على خصوصية أصحاب البيانات، سيتعين على موظفي الشركة المشاركين في معالجة المعلومات الشخصية إجراء تقييم أثر حماية البيانات ("**DPIA**"). تشمل تلك الظروف، على سبيل المثال، الحالات التي تدرس فيها الشركة ما يلي:

سياسة حماية البيانات

أ) معالجة المعلومات الشخصية على نطاق واسع يتعلق بالعديد من الأفراد أو أنواع البيانات.
ب) دمج البيانات للكشف عن معلومات شخصية جديدة عن الأفراد.
ج) معالجة المعلومات الشخصية للأفراد من الفئات المستضعفة.
د) معالجة المعلومات الشخصية الحساسة.
هـ) استخدام تقنيات جديدة قد تؤثر على الخصوصية (مثل الذكاء الاصطناعي، وتقنية التعرّف على الوجه).
و) استخدام اتخاذ القرار المؤتمت الذي قد يكون له آثار كبيرة على الأفراد.
ز) المراقبة الممنهجة للمناطق المتاحة للجمهور (مثل كاميرات المراقبة CCTV).
ح) نقل المعلومات الشخصية دوليًا بين البلدان؛ و/أو
ط) معالجة المعلومات الشخصية بطريقة تمنع ممارسة الحقوق أو الوصول إلى الخدمات.

تم توضيح عملية إجراء تقييم أثر حماية البيانات بالتفصيل في قسم موارد حماية البيانات على شبكة الشركة الداخلية، وهي تتكون من:

المرحلة الأولى: استبيان الفحص الأولي لتحديد الحاجة إلى إجراء تقييم أثر حماية البيانات.
المرحلة الثانية: تقييم أثر حماية البيانات.
المرحلة الثالثة: تفاصيل ورسم خرائط تدفق البيانات.
المرحلة الرابعة: تحديد المخاطر، والإجراءات المتفق عليها، ونموذج الاعتماد النهائي.

مشاركة المعلومات الشخصية داخل الشركة أو مع أطراف ثالثة

لا تشارك الشركة المعلومات الشخصية داخل الشركة (مثل بين الموظفين أو المقاولين) أو مع أطراف ثالثة خارج الشركة (مثل مزودي الخدمة أو المستشارين المهنيين) إلا إذا تحقق كل ما يلي:

أ) ثمة حاجة تتعلق بالأعمال لمعرفة المعلومات الشخصية ومشاركتها.
ب) تمتلك "سوبيريور" (Superior) أساسًا قانونيًا لمشاركة المعلومات الشخصية.
ج) تتوافق عملية المشاركة مع "إشعار الخصوصية" المقدم لصاحب البيانات.
د) يؤكد الفحص النافي للجهالة، وأي تقييم لأثر حماية البيانات (عند الضرورة)، وجود ضمانات تعاقدية كافية وسياسات وإجراءات لأمن البيانات قيد التنفيذ.
هـ) في الحالات التي يكون فيها الطرف الثالث معالجًا للبيانات، يتم إبرام عقد مكتوب يستوفي المتطلبات القانونية المعمول بها.
و) فيما يخص عمليات النقل عبر الحدود، يتم تنفيذ آلية نقل قانونية مناسبة.
ز) تُطبق تدابير أمنية ملائمة (مثل التشفير) في جميع الأوقات من قبل الطرف الثالث.

تُعد المعلومات الشخصية نوعًا من "السجلات المقيدة" وفقًا لسياسة الاحتفاظ بالبيانات في الشركة. بناءً على ذلك، عند التعامل مع أي مستند يحتوي على معلومات شخصية، يتوجب على موظفي الشركة حفظ المستند وتخزينه ونقله والاحتفاظ به وحذفه بما يتماشى تمامًا مع متطلبات "السجلات المقيدة" المنصوص عليها في سياسة الاحتفاظ بالبيانات.

يخضع نقل المعلومات الشخصية داخل الشركة عبر الحدود الدولية إما لاتفاقية نقل البيانات داخل المجموعة الخاصة بالشركة، أو يستند إلى قرار الكفاية الصادر عن الجهات التنظيمية لدولة معينة، والذي يدعم النقل الدولي. تتضمن اتفاقية

نقل البيانات داخل المجموعة بنودًا نموذجية معتمدة من الجهات التنظيمية، وتضمن تطبيق جميع كيانات الشركة لمستوى مناسب من الحماية لأي معلومات شخصية يتم استيرادها من كيان آخر في دولة أخرى.

سياسة حماية البيانات

الاستجابة للاختراقات والإخطار بها

لقد وضعنا إجراءات للتعامل مع أي اختراق مشتبه به للمعلومات الشخصية. وعلى وجه التحديد، طوّرت الشركة "خطة الاستجابة للحوادث الكبرى" و"خطة التعافي من الكوارث في تقنية المعلومات بالمؤسسة"، وتختبرهما بانتظام. سنقوم بإخطار أصحاب البيانات المعنيين، والعملاء، وشركاء الأعمال، والجهات التنظيمية، و/أو الأطراف الخارجية الأخرى في الحالات التي نكون فيها ملزمين قانونًا بذلك، وضمن الإطار الزمني المحدد قانونًا في حال حدوث اختراق.

إذا علمت أو اشتبهت في حدوث اختراق للمعلومات الشخصية، فعليك الاتصال بمكتب حماية البيانات فورًا عبر البريد الإلكتروني: dataprotection@superiorenergy.com.

طلبات حقوق الخصوصية

بناءً على بلد أو ولاية إقامتهم، قد يتمتع أصحاب البيانات بحقوق خصوصية معينة فيما يتعلق بكيفية تعامل الشركات مع معلوماتهم الشخصية، بما في ذلك شركة "سوبيريور" (Superior). قد تشمل هذه الحقوق، على سبيل المثال:

- الحق في الوصول.
- الحق في التصحيح.
- الحق في المحو.
- الحق في الاعتراض على المعالجة.
- الحق في تقييد المعالجة.
- الحق في الحد من معالجة المعلومات الشخصية الحساسة.
- الحق في نقل البيانات.
- الحق في اختيار عدم بيع أو مشاركة البيانات.
- الحق في رفض تقنيات اتخاذ القرار الآلي.
- الحق في سحب الموافقة.
- الحق في الإخطار باختراق البيانات.
- الحق في عدم التمييز.
- الحق في الاستئناف، بما في ذلك لدى وكالة حماية البيانات المختصة.

وللوفاء بالتزامنا بمعالجة طلبات حقوق الخصوصية هذه بطريقة مناسبة وفي الوقت المناسب، طورت الشركة نظامًا لاستلام هذه الطلبات والاستجابة لها. أولاً، يجب إرسال جميع طلبات أصحاب البيانات هذه إلى مكتب حماية البيانات باستخدام "نموذج طلبات أصحاب البيانات"، والذي يمكن الوصول إليه عبر قسم "موارد حماية البيانات" على الشبكة الداخلية للشركة (Intranet). بعد ذلك، وفور الاستلام، سيقوم الموظف المختص في مكتب حماية البيانات بمراجعة الطلب كما هو موضح في النموذج وتقديم الرد وفقًا لذلك.

حفظ السجلات

تتحمل الشركة مسؤولية الاحتفاظ بسجلات كاملة ودقيقة لجميع أنشطة معالجة المعلومات الشخصية الخاصة بنا. وبناءً عليه، سنعمل على إنشاء وصيانة سجلات لجميع أنشطة المعالجة هذه، بالإضافة إلى جميع تقييمات أثر حماية البيانات، وسجلات موافقة أصحاب البيانات، وطلبات حقوق الخصوصية والقرارات المتعلقة بها والإجراءات ذات الصلة.

سياسة حماية البيانات

التدريب والتدقيق

نطلب من جميع موظفي الشركة قراءة سياسة حماية البيانات وفهمها والالتزام بها. ولضمان الإلمام والامتثال، سيُطلب من جميع الموظفين الخضوع لتدريب منتظم يتناسب مع أدوارهم الوظيفية فيما يتعلق بسياسة حماية البيانات هذه، وسياسات وإجراءات الشركة الأخرى ذات الصلة، وقوانين والتزامات حماية البيانات المعمول بها.

القاصرون

يجوز للشركة، في ظروف محدودة، معالجة المعلومات الشخصية المتعلقة بالأطفال دون سن 18 عامًا ("القاصرون")، مثل البيانات المتعلقة بتابعي الموظفين لإدارة المزايا، أو الامتثال للالتزامات القانونية أو التنظيمية، أو البيانات المتعلقة بالمتدربين أو المهنيين الشباب الذين تستعين بهم الشركة، وفقاً لما يسمح به القانون المعمول به.

نتم أي معالجة للمعلومات الشخصية للقاصرين في امتثال صارم لقوانين حماية البيانات المعمول بها. وحيثما يقتضي القانون، ستعمل الشركة على الحصول على موافقة محددة من ولي الأمر أو الوصي القانوني قبل معالجة هذه المعلومات الشخصية.

ستضمن الشركة معالجة المعلومات الشخصية للقاصرين فقط لأغراض مشروعة ومحددة وضرورية، مع قصر ذلك على الحد الأدنى من البيانات المطلوبة، وإخضاعها لتدابير أمنية تقنية وتنظيمية معززة. لن تُستخدم هذه المعلومات لأغراض غير مناسبة، بما في ذلك الأنشطة التسويقية، ولن يتم مشاركتها مع أطراف ثالثة إلا في حالات الضرورة القصوى وبموجب تصريح قانوني.

إقرار

أقر أنا، _____ (الاسم)، بأنني في تاريخ ___ / ___ / ___20، قد استلمت نسخة من سياسة حماية البيانات الخاصة بشركة "سوبيريور" (Superior) والمخصصة للموظفين والعمال والمقاولين، وأدرك أنني مسؤول عن معرفة شروطها والالتزام بها.

التوقيع: .....

الاسم والمنصب بخط واضح: _____