



إِجَادَة
EJADA

سياسة حماية البيانات الشخصية

شركة إجادة لتحصيل ديون جهات التمويل

الموافقة والاعتماد:

الاسم	المسمى الوظيفي	التاريخ	التوقيع
ذيب المطيري	الرئيس التنفيذي	2024/07/07	

جدول المحتويات

4	التعريفات والاختصارات
1	مقدمة
2	الهدف من الوثيقة
3	نطاق السياسة
4	مبادئ حماية البيانات الشخصية
5	محتوى السياسة
5.1	الضوابط العامة
5.2	الضوابط الخاصة:
5.2.1	حقوق صاحب البيانات
5.2.2	أحكام عامة لحماية البيانات الشخصية:
5.2.3	ضوابط جمع واستخدام ونقل وإرجاع البيانات:
5.2.4	الاختيار والموافقة:
5.2.5	ضوابط استخدام وإتلاف البيانات:
5.2.6	ضوابط الوصول للبيانات:
5.2.7	الحالات المستثناة من موافقة صاحب البيانات
5.2.8	تصنيفات البيانات الشخصية

التعريفات والاختصارات

المصطلح	التعريف
الشركة	شركة إجادة لتحصيل ديون جهات التمويل
مكتب الشركة	مكتب حماية البيانات الشخصية في شركة إجادة لتحصيل ديون جهات التمويل
مجموعة البيانات	مجموعة من البيانات في موضوع معين مجمعة في قائمة أو ملف واحد
جهة التحكم	أي جهة حكومية أو جهة اعتبارية عامة مستقلة في المملكة، وأي شخصية ذات صفة طبيعية أو اعتبارية خاصة؛ تحدد الغرض من معالجة البيانات الشخصية وكيفية ذلك؛ سواء تمت معالجة البيانات بواسطتها أو عن طريق جهة المعالجة.
جهة المعالجة	أي جهة حكومية أو جهة اعتبارية عامة مستقلة في المملكة، وأي شخصية ذات صفة طبيعية أو اعتبارية خاصة؛ تعالج البيانات الشخصية لمصلحة جهة التحكم ونياً عنها.
الجهة العامة	أي جهة حكومية أو جهة اعتبارية عامة مستقلة في المملكة، أو أي من الجهات التابعة لها، وتعد في حكم الجهة العامة أي شركة تقوم بإدارة المرافق العامة، أو البنى التحتية الوطنية، أو تشغيلها، أو صيانتها، أو تقوم بمباشرة خدمة عامة فيما يخص إدارة تلك المرافق أو البنى التحتية.
البيانات الشخصية	كل بيان مهما كان مصدره أو شكله من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكناً بصفة مباشرة أو غير مباشرة، ومن ذلك: الاسم، ورقم الهوية الشخصية، والعناوين، وأرقام التواصل، وأرقام الرخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي.
البيانات	مجموعة من الحقائق في صورتها الأولية أو في صورة غير منظمّة مثل الأرقام، أو الحروف، أو الصور الثابتة، أو التسجيلات المرئية، أو التسجيلات الصوتية، أو الرموز التعبيرية
الوصول إلى البيانات	القدرة على الوصول المنطقي والمادي إلى البيانات والموارد التقنية للجهة لغرض استخدامها.
مستوى الوصول إلى البيانات	مستوى يعتمد على الأدونات والصلاحيات التي تقيد الوصول إلى البيانات والموارد التقنية على الأشخاص المصرح لهم وفقاً لما هو مطلوب لإنجاز المهام والمسؤوليات المناطة بهم.
التحقق	التأكد من هوية أي مستخدم أو عملية أو جهاز بصفته متطلباً أساسياً للسماح بالوصول إلى الموارد التقنية.
التصريح	تعريف حقوق وصلاحيات الوصول إلى البيانات والموارد التقنية لأي مستخدم أو برنامج أو عملية، والتحكم بمستويات الوصول إليها.
توافر البيانات	ضمان إمكانية الوصول المناسب والموثوق إلى البيانات واستخدامها عند الحاجة.
سرية البيانات	الحفاظ على القيود المصرح بها للوصول إلى البيانات أو الإفصاح عنها.
سلامة البيانات	حماية البيانات من أي تعديل أو إتلاف غير مصرح به نظاماً.
البيانات المحمية	البيانات المصنّفة على أنها (سري للغاية، سري، مقيد).
المعلومات العامة	البيانات بعد المعالجة – غير المحمية – التي تتلقاها أو تنتجها أو تتعامل معها الجهات العامة مهما كان مصدرها، أو شكلها أو طبيعتها.
البيانات الحساسة	البيانات التي يؤدي فقدانها أو إساءة استخدامها أو الوصول غير المصرح به إليها أو تعديلها إلى ضرر جسيم أو تأثير سلبي على المصالح الوطنية أو أنشطة الجهات الحكومية أو خصوصية الأفراد وحماية حقوقهم.
مستويات تصنيف البيانات	مستويات التصنيف المعتمدة في سياسة تصنيف البيانات وهي: "سري للغاية"، "سري"، "مقيد"، "عام"
الفرد	الشخص المتقدم بطلب الاطلاع أو الحصول على المعلومات العامة.
صاحب البيانات الشخصية	الشخص الطبيعي الذي تتعلق به البيانات الشخصية أو من يمثله أو من له الولاية الشرعية عليه.

معالجة البيانات الشخصية	جميع العمليات التي تُجرى على البيانات الشخصية بأي وسيلة كانت يدوية أو آلية، وتشمل هذه العمليات -على سبيل المثال لا الحصر- جمع البيانات ونقلها وحفظها وتخزينها ومشاركتها وإتلافها وتحليلها واستخراج أنماطها والاستنتاج منها وربطها مع بيانات أخرى.
الإفصاح عن البيانات الشخصية	تمكين أي شخص - عدا جهة التحكم - من الحصول على البيانات الشخصية أو استعمالها أو الاطلاع عليها بأي وسيلة ولأي غرض.
تسريب البيانات الشخصية	الإفصاح عن البيانات الشخصية، أو الحصول عليها، أو تمكين الوصول إليها دون تصريح أو سند نظامي، سواء بقصد أو بغير قصد.
الموافقة الضمنية	هي موافقة لا يتم منحها صراحةً من قبل صاحب البيانات، ولكنها تُمنح ضمناً عن طريق أفعال الشخص ووقائع وظروف الموقف، كتوقيع العقود أو الموافقة على الشروط والأحكام.
الأطراف الخارجية	أي جهة حكومية أو جهة اعتبارية عامة مستقلة في المملكة، وأي شخصية ذات صفة طبيعية أو اعتبارية خاصة بخلاف صاحب البيانات أو جهة التحكم أو جهة المعالجة والأشخاص المصرح لهم، تُعنى بمعالجة البيانات الشخصية.
البيانات الوصفية	هي المعلومات التي تصف البيانات وخصائصها، ومن بينها بيانات الأعمال والبيانات التقنية والتشغيلية.
البيانات المقروءة آلياً	يُقصد بها البيانات المُهيكلية بصيغة معينة يمكن قراءتها ومعالجتها آلياً باستخدام أجهزة الحاسب الآلي أو الأجهزة اللوحية وغيرها من الأجهزة.
الضوابط الأمنية	الأجهزة والإجراءات والسياسات والضمانات المادية المستخدمة لضمان سلامة البيانات وحمايتها ووسائل معالجتها والوصول إليها.
البيانات الشخصية الحساسة	كل بيان شخصي يتضمن الإشارة إلى أصل الشخص ومن في حكمه العرقي، أو القبلي، أو معتقده الديني، أو الفكري، أو السياسي، أو يدل على عضويته في جمعيات أو مؤسسات أهلية. وكذلك البيانات الجنائية والأمنية، أو بيانات السمات الحيوية التي تحدد الهوية، أو البيانات الوراثية، أو البيانات الائتمانية، أو البيانات الصحية، وبيانات تحديد الموقع، والبيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهما.
إشعار الخصوصية	هو بيان خارجي موجه للأفراد يوضح محتوى البيانات الشخصية ووسائل جمعها والغرض من معالجتها وكيفية استخدامها والجهات التي سيتم مشاركة هذه البيانات معها وفترة الاحتفاظ بها وآلية التخلص منها.
سياسة الخصوصية	هي وثيقة داخلية موجهة إلى العاملين في الجهات توضح حقوق أصحاب البيانات والالتزامات التي يجب الامتثال لها للمحافظة على خصوصية أصحاب البيانات وحماية حقوقهم.
نقل البيانات الشخصية	إرسال البيانات الشخصية إلى جهة خارج الحدود الجغرافية للمملكة - بأي وسيلة كانت - بهدف معالجتها سواء كانت بطريقة مباشرة أو غير مباشرة وفقاً لأغراض محددة مبنية على أسس نظامية، بما في ذلك النقل لأغراض أمنية، أو لحماية الصحة، أو السلامة العامة، أو تنفيذاً لاتفاقية تكون المملكة طرفاً فيها.
الموافقة الصريحة	موافقة مكتوبة أو إلكترونية تكون صريحة ومحددة وصادرة بإرادة حرة ومطلقة من صاحب البيانات تدل على قبوله لمعالجة بياناته الشخصية.
التسويق المباشر	أي اتصال، بأي وسيلة كانت، يتم عن طريقه توجيه مادة تسويقية أو دعائية إلى شخص بعينه.
النقل المباشر	نقل البيانات الشخصية من الجهة المرسله إلى الجهة المستقبلة دون مرور البيانات بأي جهة أخرى.
النقل غير المباشر	نقل البيانات الشخصية من الجهة المرسله إلى الجهة المستقبلة مروراً بجهة أخرى أو أكثر.
النقل العرضي	نقل البيانات الشخصية بشكل غير متكرر أو منتظم - عادةً ما يكون لمرة واحدة - لعدد محدود من الأشخاص، ومنها على سبيل المثال، نقل البيانات لغرض الاستفادة من خدمة في دولة أخرى لمصلحة صاحب البيانات.
قائمة الاعتماد	قائمة معتمدة من مكتب إدارة البيانات الوطنية تتضمن أسماء الدول التي تتمتع بمستوى كافٍ من الحماية لحقوق أصحاب البيانات فيما يتعلق بمعالجة بياناتهم الشخصية.
البيانات غير المعالجة	هي البيانات التي لم تخضع لعمليات متقدمة من المعالجة ويتم تبادلها في صيغتها الأولية كالبيانات الأساسية للمواطن التي يتم عرضها في بطاقة الهوية الوطنية، باستثناء المعالجة التي تفرضها الأنظمة واللوائح والسياسات لغرض مشاركة البيانات، ومنها على سبيل المثال لا الحصر، المعالجة المسبقة قبل مشاركة البيانات الشخصية كالتعميم Data Masking أو المزج Data Scrambling أو التعمية Data anonymization

منتجات البيانات (البيانات المعالجة)	يُقصد بمنتجات البيانات المُخرجات الناتجة عن تحويل البيانات بهدف خلق قيمة مضافة من خلال جمع المزيد من البيانات، أو إثرائها، أو إعدادها، أو تحليلها، أو تمثيلها، أو تصحيحها.... الخ
البيانات الحكومية	هي البيانات التي تنتجها الجهات الحكومية.
الخدمات الحكومية	الخدمات الأساسية التي تقدمها الجهات الحكومية، والتي يمكن تقديمها عن طريق طرف ثالث نيابةً عن الجهة الحكومية.
مزود البيانات	أي فرد أو جهة حكومية أو جهة خاصة تقوم بتزويد البيانات أو تقديم منتجات البيانات بمقابل مالي بشكل مباشر أو غير مباشر.
المستفيد من البيانات	أي فرد أو جهة حكومية أو جهة خاصة تقوم بطلب البيانات أو الاستفادة من منتجات البيانات بمقابل مالي.
التسويق	نشاط تبادل، أو تداول أو تزويد البيانات الخام أو البيانات المعالجة مقابل مبلغ نقدي أو قيمة عينية أخرى.
الجهة الحكومية	أي جهة حكومية أو جهة عامة مستقلة بالمملكة، أو أي من الجهات التابعة لها، ويعد في حكم الجهة الحكومية أي شركة تقوم بإدارة المرافق العامة، أو البنى التحتية الوطنية، أو تشغيلها، أو صيانتها، أو تقوم بمباشرة خدمة عامة فيما يخص إدارة تلك المرافق أو البنى التحتية.
الجهة الخاصة	أي شخصية ذات صفة اعتبارية خاصة مرخصة بالعمل في المملكة – سواء أكانت محلية أو أجنبية –، ويعد في حكم الجهة الخاصة الفرد المواطن أو المقيم بشكل رسمي في المملكة الذي يقوم بتزويد البيانات أو تقديم منتجات البيانات.
المستخدم	أي شخصية ذات صفة طبيعية أو اعتبارية تقوم بتطبيق أو استخدام أنظمة الذكاء الاصطناعي لتحقيق أهداف محددة.
صاحب البيانات	الفرد الذي تتعلق به البيانات الشخصية أو من يمثله أو من له الولاية الشرعية عليه.
عينة البيانات	البيانات التي يتم استخدامها في بناء وتدريب واختبار النماذج التنبؤية وخوارزميات الذكاء الاصطناعي للوصول إلى نتائج معينة.
مستخدم البيانات	أي شخص يمنح صلاحية الوصول إلى البيانات بغرض الاطلاع عليها أو استخدامها أو تحديثها وفقاً للمهام المصرح بها من قبل ممثل بيانات الأعمال.
ممثل بيانات أعمال	هو الشخص المسؤول عن البيانات التي يتم جمعها والاحتفاظ بها من قبل الجهة العامة التي يعمل بها، وغالباً ما يكون في مستوى إداري عالٍ، ويمكن أن يوجد في الجهة العامة أكثر من ممثل بيانات أعمال.
مختص ببيانات الأعمال	هو الشخص المسؤول عن حماية البيانات عن طريق تطبيق الضوابط المعتمدة لتصنيف البيانات بالإضافة إلى الحفاظ على الأنظمة وقواعد البيانات والخوادم التي تخزن البيانات ودعمها. وعادةً ما يكون من أعضاء إدارات تقنية المعلومات
ضوابط	ضوابط إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية
إدارة البيانات	عملية تطوير وتنفيذ الخطط والسياسات والبرامج والممارسات والإشراف عليها لتمكين الجهات من حوكمة البيانات وتعزيز قيمتها باعتبارها أحد الأصول القيمة والثمينة
أداة دليل البيانات المؤتمتة	أداة لإدارة البيانات وحوكمتها الوصفية (Meta Data) لأتمتتها ووضعها في دليل وفهرس وطني شامل للبيانات، لتمكين اكتشاف مجموعات البيانات ووصفها وتنظيمها وتحديد الجهات المنشأة للبيانات (مصدر المعلومة الصحيح) وذلك من أجل استخراج القيمة المضافة المستهدفة
بيانات الجهة العامة	البيانات قبل أو بعد المعالجة التي تتلقاها أو تنتجها أو تتعامل معها الجهات العامة مهما كان مصدرها أو شكلها أو طبيعتها
البيانات الرئيسية	مجموعة بيانات رئيسية كمصادر أساسية (بيانات الافراد-الجهات الاعتبارية-العقار...وغيره) في صورتها الأولية أو في صورة غير منظمة مثل الأرقام، أو الحروف، أو الصور، أو الفيديو، أو التسجيلات الصوتية، أو الرموز التعبيرية
البيانات المرجعية	ضوابط متفق عليها لتمثيل عناصر البيانات الأكثر شيوعاً، على سبيل المثال لا الحصر، الرموز البريدية، العملات النقدية، وأنظمة قياس درجة الحرارة (درجة مئوية أو فهرنهايت)

المصدر الموثوق	مصدر مرجعي للبيانات تم إثبات موثوقيته من خلال التحقق المسبق من صحته
بيانات غير معالجة	البيانات التي لم تخضع للمعالجة أو للتبادل بصورة أولية بأي صيغة كانت
لجنة حوكمة البيانات	هي لجنة داخلية تشكل بالجهة وهدفها مشاركة أصحاب القرار بأهمية إدارة البيانات وحماية البيانات الشخصية ونشر التوعية بالجهة
البيانات الوطنية	جميع البيانات مهما كان شكلها أو مصدرها أو طبيعتها التي يتم جمعها ومعالجتها داخل الحدود الجغرافية للمملكة وتخضع للسيادة الوطنية
السياسات والمعايير الخاصة	السياسات والمعايير المتعلقة بقطاع محدد مثل سياسات ومعايير البيانات المالية
السياسات والمعايير المشتركة	السياسات والمعايير العامة غير المرتبطة بقطاع محدد

1 مقدمة

تسعى الشركة لتنظيم معالجة البيانات الشخصية بما يكفل المحافظة على خصوصية أصحاب هذه البيانات وحماية حقوقهم عبر تطبيق مجموعة من الأحكام والإجراءات وفق الأنظمة والسياسات الوطنية.

2 الهدف من الوثيقة

نظراً للدور الذي يقوم به الشركة في النشاطات والعمليات التي تقوم بها ودورها كمتحكم ومعالج لأنواع مختلفة من البيانات التي تتضمن بيانات شخصية تبرز أهمية حماية البيانات الشخصية من خلال تطبيق الأنظمة والسياسات الوطنية ذات العلاقة لتحقيق الأهداف المتعلقة بحماية البيانات الشخصية.

3 نطاق السياسة

تنطبق أحكام سياسة حماية المعلومات على المعلومات وأنظمة معالجة المعلومات وجميع البيانات التي تتلقاها أو تنتجها أو يتعامل معها الشركة مهما كان مصدرها، أو شكلها أو طبيعتها، ويشمل ذلك السجلات الورقية ومحاضر الاجتماعات والاتصالات عبر وسائل التواصل والتطبيقات ورسائل البريد الإلكتروني والبيانات المخزنة على وسائط إلكترونية وأشرطة الصوت أو الفيديو والخرائط، والصور الفوتوغرافية والمخطوطات والوثائق المكتوبة بخط اليد وأي شكل آخر من أشكال البيانات المسجلة. وتنطبق هذه السياسة على جميع الموظفين والمقاولين والعملاء الذين يستخدمون أنظمة المعلومات والمعلومات الخاصة بالشركة.

4 مبادئ حماية البيانات الشخصية

المسؤولية:	أن يتم تحديد وتوثيق سياسات وإجراءات الخصوصية الخاصة بجهة التحكم واعتمادها من قبل المسؤول الأول بالشركة أو من يفوضه، ونشرها إلى جميع الأطراف المعنية بتطبيقها.
الشفافية:	أن يتم إعداد إشعار عن سياسات وإجراءات الخصوصية الخاصة بجهة التحكم يحدد فيه الأغراض التي من أجلها تمت معالجة البيانات الشخصية وذلك بصورة محددة وواضحة وصريحة.
الاختيار والموافقة:	أن يتم تحديد جميع الخيارات الممكنة لصاحب البيانات الشخصية والحصول على موافقته الضمنية أو الصريحة فيما يتعلق بجمع بياناته واستخدامها أو الإفصاح عنها.
الحد من جمع البيانات:	أن يقتصر جمع البيانات الشخصية على الحد الأدنى من البيانات الذي يمكن من تحقيق الأغراض المحددة في إشعار الخصوصية.
الحد من استخدام البيانات والاحتفاظ بها والتخلص منها:	أن يتم تقييد معالجة البيانات الشخصية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدّم صاحب البيانات موافقته الضمنية أو الصريحة، والاحتفاظ بها طالما كان ذلك ضرورياً لتحقيق الأغراض المحددة أو لما تقتضيه الأنظمة واللوائح والسياسات المعمول بها في المملكة وإتلافها بطريقة آمنة تمنع التسرب، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو الوصول غير المصرح به نظاماً.
الوصول إلى البيانات:	أن يتم تحديد وتوفير الوسائل التي عن طريقها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية لمراجعتها، وتحديثها، وتصحيحها.
الحد من الإفصاح عن البيانات:	أن يتم تقييد الإفصاح عن البيانات الشخصية للأطراف الخارجية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدّم صاحب البيانات موافقته الضمنية أو الصريحة.
أمن البيانات:	أن تتم حماية البيانات الشخصية من التسرب، أو التلف، أو الفقدان، أو الاختلاس، أو إساءة الاستخدام، أو التعديل، أو الوصول غير المصرح به - وفقاً لما يصدر من الهيئة الوطنية للأمن السيبراني والجهات ذات الاختصاص.
جودة البيانات:	أن يتم الاحتفاظ بالبيانات الشخصية بصورة دقيقة، وكاملة، وذات علاقة مباشرة بالأغراض المحددة في إشعار الخصوصية.
المراقبة والامتثال:	أن تتم مراقبة الامتثال لسياسات وإجراءات الخصوصية الخاصة بجهة التحكم، ومعالجة الاستفسارات والشكاوى والنزاعات المتعلقة بالخصوصية.

5 محتوى السياسة

5.1 الضوابط العامة

#	البند
1	تاريخ فعالية السياسة: يبدأ سريان هذه السياسة اعتباراً من تاريخ الموافقة على هذه الوثيقة المشار إليه بالتوقيعات الواردة في جدول الموافقة. ويتم نشر نسخة معتمدة من الوثيقة من قبل مكتب الشركة.
2	جدول مراجعة السياسة: نظراً لطبيعة التسارع في التطور التقني ومتطلبات التغيير في الأعمال فإنه هذه السياسة يجب المراجعة الدورية للسياسة وتحديثها بما يعكس أي تغييرات طرأت أو يعكس تحسين أحكام هذه السياسة بما يمنح حقاً أفضل لصاحب البيانات الشخصية. ويجب أن تتم المراجعة من مكتب الشركة وتعتمد من معالي رئيس الشركة أو من يفوضه.
3	مراقبة الامتثال: يقاس الامتثال لسياسة حماية البيانات الشخصية وفقاً لمعايير ومؤشرات الأداء الموضوعة من مكتب الشركة وبالتوافق مع متطلبات مكتب إدارة البيانات الوطنية ويتم مراجعة معايير الامتثال بشكل دوري من قبل مدير المكتب. وأن يكون مكتب الشركة مسؤول تحديد وتوثيق الإجراءات التصحيحية التي سيتم اتخاذها في حال عدم الامتثال للسياسة.

5.2 الضوابط الخاصة:

5.2.1 حقوق صاحب البيانات

#	الحقوق
1	على الشركة أن تطرح وسائل لاستقبال طلبات أصحاب البيانات والاستجابة لها.
2	على الشركة أن تطلع أصحاب البيانات على حقوقهم التالية: ● الحق في العلم ويشمل إشعاره بالأساس النظامي أو الاحتياج الفعلي لجمع بياناته الشخصية. ● الحق في الرجوع عن موافقته على معالجة بياناته الشخصية أو تقييد المعالجة. مالم يكن هناك أغراض مشروعة تتطلب عكس ذلك. ● الحق في الوصول إلى البيانات والحصول، على نسخة منها بصيغة واضحة. ● الحق في التصحيح أو التحديث. ● الحق في الإزالة ما انتهت الحاجة إليه. ● الحق في الاعتراض

5.2.2 أحكام عامة لحماية البيانات الشخصية:

#	الضوابط
1	يجب أن يكون هناك إجراء موثق ورسمي للتعامل مع أي استفسارات وشكاوى تتعلق بخصوصية البيانات ويجب أن تكون واضحة على مستوى الشركة.
2	أن يكون هناك برنامج مستمر للتحقق من الالتزام بمعايير نظام حماية البيانات الشخصية ويجب أن يتم التعريف بهذا البرنامج على مستوى الشركة لمعرفة وتقييم ورفع التقارير ومراقبة التقدم الحاصل في الالتزام بمعايير نظام حماية البيانات الشخصية ضمن الشركة.
3	عملية معالجة البيانات وحاجة الأعمال لتلك البيانات يجب أن تكون موثقة ويتم الحفاظ عليها.
4	يجب على مكتب الشركة تطوير وتطبيق سياسة لتصنيف البيانات وتؤكد من أن كافة البيانات الموجودة تملكها أو تتعامل معها تم تصنيفها بناء على تلك السياسة.
5	يجب تصنيف الأصول التي تقوم على معالجة البيانات بدرجة تصنيف تماثل درجة تصنيف البيانات التي يتم جمع ومعالجة ونقل البيانات من خلالها.
6	يجب تطبيق متطلبات حماية البيانات الشخصية الخاصة بكل تصنيف للبيانات الواردة في نظام حماية البيانات الشخصية.
7	يجب التحقق من أن يتم العمل بالإجراءات الملائمة لضمان جودة البيانات مثل المراجعة الدورية والتدقيق للتأكد من أن كل البيانات يتم حفظها بأحدث صيغة.
8	البيانات التي يتم الحصول على إذن باستخدامها يجب أن تستخدم فقط في حدود الطلب والغرض الذي منحت من أجله.

5.2.3 ضوابط جمع واستخدام ونقل وإرجاع البيانات:

#	الضوابط
1	يجب معالجة البيانات فقط لحاجة العمل ووفق ما تسمح به الأنظمة لذلك.
2	في حال جمع البيانات يجب أن يتم حفظها في المدة التي وردت في سياسة النسخ الاحتياطي لإدارة الأمن السيبراني ويجب ألا تتجاوز المدة المحددة.
3	يجب جمع الحد الأدنى فقط من البيانات الشخصية الذي يسمح بأداء العمل الذي جمعت من أجله
4	في الحالات التي تكون فيها الشركة هي جهة التحكم فإن أي إجراءات لجمع البيانات الشخصية يجب اعتمادها من قبل المسؤولين عن البيانات الشخصية في الشركة قبل تطبيقها لضمان أن البيانات الشخصية يتم جمعها تمت بشكل مناسب
5	يجب تقييم البيانات التي سيتم جمعها من الأطراف الخارجية بشكل كاف لضمان أن الإجراءات التي تمت من ذلك الطرف تمت بشكل نظامي الإشعار
6	في حال كانت الشركة يقوم بدور جهة المعالجة نيابة عن جهة أخرى تمثل جهة التحكم، فعلى تلك الجهة إشعار أصحاب البيانات بشكل رسمي بما يلي: • وصف أنواع البيانات الشخصية التي تم جمعها عن صاحب البيانات وطرق جمعها والمصادر التي تم جمعها منها، وبأي شيء استخدمت من أجله، والبيانات التي تم حفظها أو تم إفصاحها للغير. • التأكيد على أن البيانات الشخصية الخاصة بصاحب البيانات ستستخدم فقط من أجل الأغراض التي تم جمعها من أجلها وذكرها في إشعار جمع البيانات. • إشعار أصحاب البيانات بأنهم هم المسؤولين (في حال جمع البيانات منهم مباشرة) عن صحة بياناتهم شخصية ودقتها، ويجب توضيح إجراءات وصول صاحب البيانات إلى بياناته الشخصية لتحديثها أو تعديلها. • إشعار صاحب البيانات الشخصية عن الإجراءات التي ستتم لمواجهة أي تسرب حصل لبياناته. وإبلاغ الجهة المختصة عن تلك الحادثة.

- في حال كانت الشركة يقوم بدور جهة التحكم، عليها إشعار أصحاب البيانات بشكل رسمي بما يلي:
- وصف أنواع البيانات الشخصية التي تم جمعها عن صاحب البيانات وطرق جمعها والمصادر التي تم جمعها منها، وبأي شيء استخدمت لأجله، والبيانات التي تم حفظها أو تم إفصاحها للغير.
 - التأكيد على أن البيانات الشخصية الخاصة بصاحب البيانات ستستخدم فقط من أجل الأغراض التي تم جمعها من أجلها وذكرها في إشعار جمع البيانات.
 - إشعار أصحاب البيانات عن الجهات والأطراف الخارجية التي ستقوم بمعالجة بياناتهم كجهات معالجة ولأي غرض سيتم ذلك.
 - إشعار أصحاب البيانات عن الضوابط التي يلتزم بها الشركة لحماية البيانات الشخصية لأصحاب البيانات.
 - إشعار صاحب البيانات بطريقة التواصل مع الشركة للتقدم بشكوى رسمية تجاه أي إجراء يتعلق بحماية بياناته الشخصية.
 - إشعار أصحاب البيانات بأنهم هم المسؤولون (في حال جمع البيانات منهم مباشرة) عن صحة بياناتهم شخصية ودقتها، ويجب توضيح إجراءات وصول صاحب البيانات إلى بياناته الشخصية لتحديثها أو تعديلها.
 - إشعار صاحب البيانات الشخصية عن الإجراءات التي ستتم لمواجهة أي تسرب حصل لبياناته، وإبلاغ الجهة المختصة عن تلك الحادثة.
 - إشعار إدارة الأمن السيبراني عن تسريب أي بيانات شخصية وإبلاغهم بشكل رسمي عن الحادثة.

7

5.2.4 الاختيار والموافقة:

في حال كانت الشركة يمثل جهة التحكم فيجب عليها عند طلب الموافقة من صاحب البيانات الالتزام بما يلي (وذلك في غير الاستثناءات الواردة في الفقرة 7 من احكام السياسة):

#	الضوابط
1	يجب أن يتم إبلاغ صاحب البيانات قبل جمع بياناته الشخصية بالخيارات المتاحة له في البيانات المراد جمعها واستخدامها وإفصاحها والغرض الذي جمعت من أجله والموافقة المطلوبة منه.
2	في حال كان التعامل مع البيانات الحساسة (الفقرة 8 من أحكام السياسة) لغرض جمعها واستخدامها وإفصاحها، عندها يجب أخذ موافقة كتابية من صاحب البيانات قبل جمعها.
3	يجب أخذ الموافقة من صاحب البيانات عند أي تغييرات ستتم على معالجة بياناته.

وفي حال كانت الشركة يمثل جهة المعالجة فيجب عليها الالتزام بما يلي:

#	الضوابط
1	التحقق من توافر موافقة صاحب البيانات الشخصية على معالجة هذه البيانات وأن يكون شكل الموافقة يتناسب مع نوع البيانات المراد معالجتها (مثل وجود موافقة كتابية للبيانات الانتمانية).
2	يجب أخذ الموافقة من صاحب البيانات عند أي تغييرات ستتم على معالجة بياناته.
3	يحق لصاحب البيانات تقديم اعتراضه لأسباب مشروعة على معالجة بياناته

5.2.5 ضوابط استخدام وإتلاف البيانات:

#	الضوابط
1	يجب استخدام البيانات التي تم جمعها في حدود الاستخدامات التي تم ذكرها في الإشعارات ذات العلاقة، وبحدود ما يسمح به النظام.
2	لا يجب الاحتفاظ بالبيانات الشخصية لمدة تتجاوز الحاجة لها التي تم ذكرها في وثيقة الإشعار ما لم يكن هناك نص نظامي يسمح بذلك. ومن غير المقبول الاحتفاظ بالبيانات لغرض "في حال دعت الحاجة إليها"
3	البيانات الشخصية (الأصلية أو المؤرشفة أو المحفوظة في نسخ احتياطية) التي لم يعد هناك حاجة لحفظها يجب تعميمها أو إتلافها بطريقة تمنع ضياعها، أو سرقتها، أو إساءة استخدامها، أو الوصول غير المسموح لها
4	أي طرف ثالث يكون طرفاً في عملية إتلاف البيانات يجب اعتباره جهة معالجة وتنطبق عليه كافة الإجراءات الواردة في هذه السياسة
5	لا يجوز استخدام البيانات الشخصية لغرض تجربة تطوير على أنظمة حالية إلا في حال كانت تلك البيانات تم تعميمها بشكل لا يمكن معه تحديد هوية صاحب البيانات الشخصية.
6	لحساسية البيانات الشخصية يجب الاهتمام بتأمين وحماية شكلها ووسائط تخزينها وطريقة نقلها بشكل كاف منطقياً وفيزيائياً من إساءة الاستخدام والضياع والوصول غير المسموح به والتسريب، والتعديل، وإتلاف، والتغيير.
7	يجب أن يتم نقل البيانات بشكل مشفر بما يتماشى مع سياسة التشفير المتبعة لدى الشركة .

5.2.6 ضوابط الوصول للبيانات:

#	الضوابط
1	يجب تطوير نموذج طلب الوصول إلى البيانات الشخصية وتوضيح إجراءاته، ويجب أن تكون عملية الطلب واضحة وتطلب ضمن الشركة لضمان أن الاستجابة لمثل تلك الطلبات مستقرة وعادلة ومفهومة ويتم الاستجابة عليها بطريقة ملائمة وفي زمن معقول

- 2 الأفراد الذين يقومون بتقديم طلب الوصول للبيانات الشخصية، يجب يتم التحقق منهم بشكل ملائم قبل قبول طلباتهم
- 3 يجب التوقيع على وثيقة عدم إفشاء سرية قبل أن يمكن للموظف الوصول إلى البيانات الشخصية
- 4 يجب توقيع وثيقة عدم إفشاء سرية من قبل أي طرف ثالث يتعامل مع الشركة في حال كانت طبيعة التعامل معه تتيح له صلاحية الوصول إلى البيانات الشخصية.
- 5 يجب أن يتم منح صلاحية الوصول إلى البيانات بناء على قدر الحاجة للمعرفة وبمبدأ الحد الأدنى من الصلاحيات
- 6 يجب على مدراء قواعد البيانات عدم السماح بحذف أي بيانات حساسة من قواعد البيانات إلا بعد الحصول على الموافقة من عدة مستويات مخولة بذلك وتشمل مالك البيانات الشركة.
- 7 يجب أن يتم مراجعة سجلات عمليات إدارة البيانات بشكل دوري بما يتماشى مع إجراءات صلاحيات الوصول ذات العلاقة بالشركة .

5.2.7 الحالات المستثناة من موافقة صاحب البيانات

#	الضوابط
1	يستثنى من أحكام هذا النظام كل مما يلي: إذا كانت البيانات الشخصية متاحة للعموم، أو جرى جمعها من مصدر متاح للعموم.
2	إذا كانت الشركة في دور جهة التحكم، وكان جمع البيانات الشخصية من غير صاحبها مباشرة، أو معالجتها لغرض آخر غير الذي جمعت من أجله مطلوباً لأغراض أمنية أو لتنفيذ نظام آخر أو الاستيفاء متطلبات قضائية.
3	إذا كان التقييد بهذا الحظر قد يلحق ضرراً بصاحب البيانات الشخصية أو يؤثر على مصالحه الحيوية.
4	إذا كان جمع البيانات الشخصية أو معالجتها ضرورياً لحماية الصحة، أو السلامة العامة، أو حماية حياة فرد، أو أفراد معينين، أو حماية صحتهم .
5	إذا كانت البيانات الشخصية لن تُسجل أو تُحفظ في صيغة تجعل من الممكن تحديد هوية صاحبها ومعرفته بصورة مباشرة أو غير مباشرة.

5.2.8 تصنيفات البيانات الشخصية

#	الضوابط
1	البيانات غير الشخصية (Impersonal Data) هي البيانات والمعلومات التي لا يمكن التعرف منها بشكل مباشر على الشخص صاحب البيانات، ولكن من خلال مجموعة من تلك البيانات فإنه من الممكن تحديد هوية صاحب البيانات بشكل غير مباشر.
2	البيانات الشخصية (Personal Data) هي البيانات والمعلومات التي يمكن التعرف منها بشكل مباشر أو غير مباشر على الشخص صاحب البيانات، وذلك على سبيل المثال: ● الاسم ● تاريخ الميلاد ● الجنسية

- رقم الهوية
- عنوان المنزل
- رقم الجواز

البيانات الشخصية الحساسة

3 هي البيانات والمعلومات التي يمكن التعرف منها بشكل مباشر أو غير مباشر على الشخص صاحب البيانات، ولكن قد يتسبب الإفصاح عنها بضرر كبير على صاحب البيانات مثل البيانات الانتمائية.
