CITRA

الهيئة العامة للاتصالات و تقنية المعلومات

COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

لائحة حماية خصوصية البيانات

Data Privacy Protection Bylaw

النسخة التجريبية

Beta Version

أغسطس 2023

Beta Version

المحتويات

المقدمة 1
التعريفات والمصطلحات الفنية 1-2
المادة الأولى: نطاق اللائحة 2
المادة الثانية: شروط جمع ومعالجة البيانات الشخصية 2
المادة الثالثة: مشروعية جمع ومعالجة البيانات 3
المادة الرابعة: شروط جمع ومعالجة البيانات 3-4
المادة الخامسة: أمن وحماية البيانات الشخصية 4-5
المادة السادسة: الإخطار عند حدوث الإختراقات 6
المادة السابعة: أحكام عامة 6

Beta Version

المقدمة

يتزايد الطلب على خدمات الاتصالات وتقنية المعلومات من قبل القطاعين العام والخاص التي يوفرها مقدمي هذه الخدمات في دولة الكويت باستخدام تقنيات متطورة، كحلول الحوسبة السحابية (Cloud Computing) وإنترنت الأشياء وغيرها، ولما تقدمه هذه الخدمات من مميزات تعتمد على موارد البنية التشغيلية والبرمجيات وغيرها من عناصر تقنية المعلومات التي يوفرها ويشغلها مقدمي خدمات الاتصالات وتقنية المعلومات، وتشمل عمليات جمع، ومعالجة لبيانات ومحتويات المستخدم.

حيث أن الهيئة العامة للاتصالات وتقنية المعلومات تعي ضرورة أن يلتزم مقدمي خدمات الاتصالات وتقنية المعلومات بحماية البيانات والحقوق والحريات الأساسية للنقل المتعلقة بخصوصية البيانات الشخصية المجمعة، مما يحفز الهيئة أن تصدر مجموعة من الأدوات التنظيمية تتضمن الشروط والأسس والتوجيهات التي تتعلق بتنظيم ممارسات إدارة ومعالجة البيانات من قبل مقدمي خدمات الاتصالات وتقنية المعلومات وكل ما يرتبط بها من أحكام وإلتزامات لدعم هذا التوجه التنظيمي.

وكما أن الهيئة العامة للاتصالات وتقنية المعلومات تطمح لتطوير صناعة متينة تعتمد على توفير أفضل خدمات الاتصالات وتقنية المعلومات بغرض تقديمها للجهات الحكومية وقطاع الأعمال والأفراد داخل دولة الكويت، مما يدعم عمل الأنشطة الحكومية والتجارية والصناعية، ويسهم نحو استقطاب المستثمرين المهتمين بهذا المجال وتعزيز أسس تنافسية تحقيقاً لرؤية دولة الكويت نحو النهوض بها إلى مركز مالي وتجاري (كويت جديدة 2035).

التعريفات والمصطلحات الفنية

يكون للكلمات والعبارات التالية حيثما وردت في هذا الدليل المعاني المخصصة لها أدناه، كما تعتمد التعاريف الواردة في قانون الهيئة العامة للاتصالات وتقنية المعلومات ولائحته التنفيذية:

الهيئة: الهيئة العامة للاتصالات وتقنية المعلومات بموجب القانون رقم (37) لسنه 2014 والمعدل بالقانون رقم (98) لسنة 2015، ولائحته التنفيذية.

مقدم الخدمة/ المرخص له: الشخص الذي يرخص له بتقديم خدمة أو أكثر من خدمات الاتصالات للجمهور، أو يرخص له بإدارة، أو إنشاء، أو تشغيل شبكة اتصالات، أو خدمة الإنترنت لتوفير خدمات الاتصالات للجمهور، يشمل مقدمي المعلومات أو المحتوى التي تقدم بواسطة شبكة الاتصالات.

الشخص الاعتباري: هو كيان ذاتي مستقل لتحقيق غرض معين ويتمتع بالشخصية القانونية في حدود هذا الغرض، وينطبق على الشركات أو الكيانات المؤسسية الخاصة أو العامة التي تملكها الدولة أو المنظمات والتي لديها موطن في دولة الكويت.

البيانات الشخصية: هي البيانات ذات صلة بشخص طبيعي أو شخص اعتباري محدد الهوية أو يمكن تحديده من خلال هذه البيانات بطريقة مباشرة كتحديد الإسم والهوية، أو المعلومات المالية، أو الصحية، أو العرقية، أو الدينية أو أي بيانات تسمح بتحديد الموقع الجغرافي للشخص أو البصمة الشخصية أو البصمة الوراثية، أو من خلال الجمع بين البيانات المتوفرة وأية بيانات

Beta Version

أخرى، أو أي ملف صوتي بما في ذلك صوت الشخص، وأي معرف آخر يسمح بالاتصال عبر الإنترنت بالشخص.

المستفيد/ المستخدم: الشخص الذي يستفيد من خدمة الاتصالات العامة أو التي يقصد استخدامها في أغراض خاصة باستخدام عمليات الاتصال.

جمع ومعالجة البيانات: أي عملية أو مجموعة من العمليات يتم اتخاذها على البيانات الشخصية سواء كانت داخل دولة الكويت أو خارجها باستخدام الوسائل الآلية أو وسائل أخرى مثل جمع، تسجيل، تنظيم، تحليل، تخزين، أو تعديل، استرجاع، استخدام أو الإفصاح من خلال الإرسال والنشر أو جعلها متاحة، دمجها، تقييدها، حذفها أو إتلافها.

إزالة وحذف البيانات: عملية أو مجموعة عمليات يتخذها المرخص له/مقدم الخدمة بهدف التوقف عن استخدام بيانات العميل للأغراض التجارية وعدم إتاحتها للعامة مع جواز استمراره بالاحتفاظ بتلك البيانات واستخدامها للأغراض الأمنية ولتنفيذ القرارات والأحكام القضائية والمطالبات المالية الناتجة عن عقد الاشتراك المبرم بين المستفيد/المستخدم ومقدم الخدمة / المرخص له فقط.

الطرف الثالث: هو أي شخص طبيعي أو اعتباري يقوم بجمع أو معالجة البيانات الشخصية بالنيابة عن مقدم الخدمة وبتوجيه منه سواء كان ذلك بشكل مباشر أو غير مباشر.

المادة الأولى: نطاق اللائحة

تطبق هذه اللائحة على جميع مقدمي الخدمة المرخص لهم من قبل الهيئة، الذين يعملون على جمع، معالجة، وتخزين البيانات الشخصية ومحتوى بيانات المستخدمين كليا أو جزئيا، سواء بشكل دائم أو مؤقت بالوسائل الآلية أو بأي وسائل أخرى والتي تشكل جزءا من نظام حفظ البيانات، سواء تمت المعالجة داخل دولة الكويت أو خارجها.

ولا تطبق أحكام هذه اللائحة على الممارسات المتعلقة بالتحريات الأمنية ورصد المخالفات أو الممارسات المخالفة للقوانين والقرارات والأحكام القضائية والمطالبات المالية الناشئة عن عقد الاشتراك.

المادة الثانية: شروط جمع ومعالجة البيانات الشخصية

يجب علي مقدم الخدمة وقبل توفير الخدمة للمستخدم أن يقوم بالتالي:

1) توفير كافة معلومات وشروط الخدمة وطلب تغيير أو إلغاء البيانات، موضحة وبعبارات سهلة، وأن تتوفر باللغتين الإنجليزية والعربية.

2) الحصول على موافقة طالب الخدمة على جمع أو معالجة البيانات الشخصية وعلمه وقبوله بجميع الشروط والإلتزامات وأحكام جمع ومعالجة البيانات.

3) توضيح الغرض من جمع بيانات المستخدم الشخصية واللازمة لتقديم الخدمة وكيفية استخدام هذه البيانات.

Beta Version

المادة الثالثة: مشروعية جمع ومعالجة البيانات

لا تكون جمع ومعالجة البيانات مشروعة وقانونية إلا في حال توافر إحدى الحالات التالية:

1) الحصول على موافقة المستخدم صاحب البيانات.

2) أن تكون ضرورية للامتثال لإلتزام قانوني يخضع له مقدم الخدمة.

3) أن تكون ضرورية لحماية بيانات المستخدم.

4) إذا كانت الأغراض التي يقوم بها مقدم الخدمة تتطلب تحديد هوية صاحب البيانات.

5) الحصول على موافقة خطية من قبل ولي أمر القاصر إذا كان عمره أقل من (18) سنة.

وفي جميع الأحوال يجب أن يكون لمقدم الخدمة القدرة على إثبات موافقة صاحب البيانات على معالجة البيانات.

المادة الرابعة: شروط جمع ومعالجة البيانات

يجب على مقدم الخدمة أثناء توفير الخدمة أو بعد انتهائها أن يقوم بجمع ومعالجة البيانات وفقا للشروط التالية:

1) تقديم معلومات واضحة يسهل الوصول إليها حول ممارساتهم وسياساتهم فيما يتعلق بالبيانات الشخصية لضمان إجراء عمليات الجمع والمعالجة وبشفافية.

2) تحديد الغرض من جمع البيانات والأساس القانوني لمعالجة البيانات وفترة الاحتفاظ بها إن وجدت.

3) تحديد هوية ومكان مقدم الخدمة، بما في ذلك معلومات عن كيفية الاتصال بهم بشأن ممارساتهم ومعالجة البيانات الشخصية.

4) معالجة البيانات بطريقة تضمن حماية البيانات الشخصية من المعالجة غير المصرح بها أو المعالجة غير القانونية وضد الخسارة العارضة والتلف أو الإضرار بها وذلك باستخدام التدابير الفنية والتنظيمية المناسبة ("السلامة والسرية").

5) يجب على مقدم الخدمة إخطار الهيئة في حال كشف بيانات المستخدمين الشخصية لأي شركة زميلة أو مالكة لمقدم الخدمة أو طرف ثالث بشكل مباشر أو غير مباشر، على أن يكون مقدم الخدمة هو المسؤول عن حماية خصوصية البيانات المشارك فيها.

6) استخدام الوسائل التكنولوجية المناسبة التي تمكن المستخدمين من ممارسة حقهم في الوصول إلى البيانات الشخصية ومراجعتها وتصحيحها بشكل مباشر، ويتعين على مقدم الخدمة منح الطرف الثالث (إن وجد) كافة الصلاحيات الضرورية والتنظيمية لاستخدام أي برامج، أو أي أعمال ملكية فكرية أخرى يحميها النظام.

7) تقديم معلومات عن مكان تخزين البيانات الشخصية في حال كانت داخل أو خارج دولة الكويت.

8) تحديد آلية الحصول على أو تصحيح أو إزالة البيانات الشخصية أو تقييد الوصول إليها أو معالجتها، أو الاعتراض على معالجتها أو طلب نقل البيانات الشخصية.

Beta Version

9) إخطار صاحب البيانات في حال كان مقدم الخدمة يعتزم نقل بياناته الشخصية إلى خارج دولة الكويت.

10) إزالة البيانات الشخصية التي بحوزته حال انتهاء العلاقة التعاقدية مع صاحب البيانات.

11) الحصول على موافقة صاحب البيانات قبل الكشف عن بياناته الشخصية لأي طرف ثالث لأغراض تسويقية لا تتعلق مباشرة بتوفير خدمات الاتصالات وتقنية المعلومات التي يطلبها المستخدم.

12) يجب على مقدم الخدمة، أن يوفر وسيلة سهلة الاستخدام، وعملية ويمكن النفاذ إليها بسهولة تمكن المستخدم من تعديل بياناته، أو سحب موافقته، أو تعطيل خدمة، أو طريقة جمع، أو استخدام، أو معالجة أو الإفصاح عن بياناته الشخصية

13) يجب على مقدم الخدمة إزالة البيانات الشخصية للمستخدم إذا:

أ) قام المستخدم بسحب الموافقة الخاصة بمعالجة أو استخدام البيانات الشخصية.

ب) لم تعد البيانات الشخصية لازمة لتقديم الخدمات التي يطلبها المستخدم.

ج) لم يعد المستخدم مشتركا في الخدمة التي تم جمع البيانات الشخصية بشأنها.

14) يجب على مقدم الخدمة إنشاء والحفاظ على سياسة خصوصية مكتوبة بحيث:

أ) تبين بالتفصيل عمليات وإجراءات مقدم الخدمة فيما يتعلق بجمع واستخدام والإفصاح عن البيانات الشخصية، بما في ذلك الطريقة التي سوف يتبعها للامتثال.

ب) يتم نشرها على الموقع الإلكتروني لمقدم الخدمة وتقدم للمستخدمين عند التعاقد في الخدمات.

15) إذا تم الكشف عن البيانات الشخصية المخزنة من قبل مقدم الخدمة بشكل غير صحيح وأدى هذا الكشف أو النفاذ إلى إلحاق الضرر بعدد كبير من المستخدمين، وجب على مقدم الخدمة إخطار الهيئة والمستخدمين وجهات إنفاذ القانون في أقرب وقت ممكن وبما لا يزيد في أي حال عن (72) ساعة.

16) عند إعداد أي عملية أو نظام أو إجراءات لتوفير تسهيلات أو خدمات الاتصالات، يجب على مقدم الخدمة أن يعتمد الخصوصية من خلال تصميم الخدمات.

المادة الخامسة: أمن وحماية البيانات الشخصية

على مقدم الخدمة اتخاذ الآتي:

1) توفير التدابير الأمنية المناسبة لحماية البيانات الشخصية للمستخدم ضد الخسارة، الضرر، الإفصاح أو الإختراق من طرف آخر غير مصرح له أو استبدال البيانات أو المعلومات بأخرى غير صحيحة أو إضافة معلومات غير صحيحة. ويجب أن تكون هذه التدابير ملائمة لطبيعة ونطاق أنشطته وحساسية أي بيانات شخصية يتم جمعها وتخزينها، بما في ذلك الأمور التالية:

أ) معالجة وتشفير البيانات الشخصية، وتبعا لمستوى البيانات المحددة بسياسة تصنيف البيانات لمقدم الخدمة.

Beta Version

ب) ضمان السرية المستمرة ونزاهة وتوافر ومرونة نظم وخدمات المعالجة.

ج) استعادة التوافر والوصول إلى البيانات الشخصية في الوقت المناسب في حالة وقوع قوة قاهرة.

د) اختبار وتقييم فعالية التدابير التقنية والتنظيمية لضمان أمن المعالجة.

2) تأمين البيانات من التدمير العرضي، غير القانوني، الفقد، و/ أو التغيير أو الكشف غير المصرح به أو الوصول إلى البيانات الشخصية المرسلة أو المخزنة أو التي تتم معالجتها بطرق أخرى.

3) الإلتزام بالسياسات والممارسات العالمية المتعلقة باستمرارية الأعمال، والتعافي من الكوارث، وإدارة المخاطر، وسياسات أمن المعلومات.

4) الاحتفاظ بسجلات أنشطة المعالجة وأن تتضمن السجلات كافة المعلومات التالية:

أ) إسم وبيانات الاتصال بمقدم الخدمة، وممثله إذا كان خارج دولة الكويت ومسؤول حماية البيانات.

ب) أغراض معالجة البيانات.

ج) وصف فئات أصحاب البيانات وفئات البيانات الشخصية الأخرى.

د) نقل البيانات الشخصية، إذا لزم الأمر، إلى خارج دولة الكويت مع تحديد هوية هذه الدولة.

ه) وصف عام للتدابير الأمنية الفنية والتنظيمية المستخدمة.

5) إتاحة السجلات للاطلاع عليها من قبل الهيئة عند الطلب.

6) مراعاة الضوابط الخاصة بتصميم أو تغيير أو تطوير المنتجات والنظم والخدمات والتي من الممكن أن تؤثر على معالجة البيانات الشخصية.

7) تطوير والإلتزام بسياسات داخلية للحماية وخصوصية البيانات.

8) تحديد وتدريب وتوعية المسؤولين عن حماية البيانات الشخصية.

9) وضع نظم داخلية لتلقي الشكاوى ودراستها على مدار الساعة، وطلبات الوصول للبيانات، وطلبات تصحيحها أو حذفها.

10) وضع نظم داخلية للإدارة الفعالة للبيانات الشخصية، والإبلاغ عن أي تجاوز للإجراءات التي تهدف إلى حمايتها.

11) إجراء عمليات تدقيق ومراجعة شاملة عن مدى الإلتزام بحماية البيانات الشخصية.

12) إخطار الهيئة العامة للاتصالات وتقنية المعلومات بحال حدوث إختراقات للبيانات الشخصية.

Beta Version

المادة السادسة: الإخطار عند حدوث الإختراقات

1) على مقدم الخدمة عند حدوث إختراق للبيانات الشخصية وفي مدة لا تتجاوز (72) ساعة بعد علمها إخطار حدوث إختراق للبيانات الشخصية إلى الهيئة العامة للاتصالات وتقنية المعلومات.

2) يتضمن الإخطار:

أ) طبيعة الإختراق، ومدى تسرب البيانات الشخصية والأشخاص المسربة معلوماتها والمستويات الأمنية المتضررة.

ب) إسم وآلية التواصل مع مسؤول حماية البيانات.

ج) النتائج المحتملة للإختراق، والتدابير المتخذة أو التي يقترح أن يتخذها مقدم الخدمة لمعالجة الإختراق.

د) إخطار صاحب البيانات الشخصية بحال حدوث إختراقات للبيانات الشخصية.

3) لا يلزم إبلاغ صاحب البيانات إذا قام مقدم الخدمة باتخاذ تدابير الحماية الفنية والتنظيمية المناسبة، وتم تطبيق هذه التدابير على البيانات الشخصية المتأثرة بحدوث الإختراق.

4) اتخاذ التدابير اللاحقة التي تكفل عدم إرتفاع المخاطر على حقوق وحريات الأشخاص أصحاب البيانات.

المادة السابعة: أحكام عامة

1) على جميع مقدمي الخدمة أو المصرح لهم بامتلاك شبكات اتصالات عامة توفيق أوضاعهم مع أحكام هذه اللائحة واللوائح الاخرى ذات العلاقة مع هذه اللائحة والصادرة عن الهيئة خلال مدة لا تتجاوز سنة من تاريخ نشرها.

2) يجوز للهيئة إصدار تعليمات أو إرشادات متعلقة بخصوصية البيانات كلما اقتضى الحال ذلك.

3) للهيئة في حال ثبوت مخالفة أحكام هذه اللائحة أو قوانين دولة الكويت تطبيق الجزاءات والغرامات المنصوص عليها في قانون إنشاء الهيئة العامة للاتصالات وتقنية المعلومات رقم (37) لسنة 2014 والمعدل بالقانون رقم (98) لسنة 2015.