

الهيئة السعودية للمواصفات والمقاييس والجودة
Saudi Standards, Metrology and Quality Org. (SASO)



SASO FDS *****

إدارة البيانات – حماية البيانات الشخصية
Data Management – Personal Data Protection

ICS ***

المقدمة

قامت الهيئة السعودية للمواصفات والمقاييس والجودة بإعداد المواصفات القياسية لمجال حماية البيانات الشخصية بالتعاون مع الهيئة السعودية للبيانات والذكاء الاصطناعي والتي ستدعم آلية حفظ البيانات على أجهزة ووسائل تخضع للتدابير اللازمة لتوفير البيانات بسهولة.

المحتويات

٢	المقدمة
٤	١/ المجال
٤	٢/ المراجع التكميلية
٤	٣/ المصطلحات والتعاريف
٤	١/٣ البيانات الشخصية
٤	٤/٣ بيانات غير معالجة
٤	٥/٣ المكتب
٤	٦/٣ لجنة حوكمة البيانات
٤	٧/٣ النظام
٤	٨/٣ اللوائح
٥	٩/٣ المعالجة
٥	١٠/٣ الجهة المختصة
٥	٤ التخطيط
٥	١/٤ التقييم المبدئي لحماية البيانات الشخصية
٥	٢/٤ خطة حماية البيانات الشخصية
٦	٥ التدريب والتوعية
٦	١/٥ التدريب على حماية البيانات الشخصية
٧	٦ تسريب البيانات
٧	١/٦ الإشعار بتسريب البيانات
٧	٢/٦ إدارة التعامل مع تسريب البيانات
٨	٧ إدارة دورة حياة البيانات
٨	١/٧ الإشعارات بحماية البيانات الشخصية وإدارة الموافقة
٨	٢/٧ حقوق صاحب البيانات
٩	٢/٧ تقييم مخاطر حماية البيانات الشخصية
٩	٣/٧ مراقبة وتدقيق الامتثال
٩	٨ السجلات
١٠	المراجع

١/ المجال.

تحتوي هذه المواصفة القياسية في مجال حماية البيانات الشخصية على التخطيط لإعداد خطة متكاملة للحماية، والتقييم المبدئي للمخاطر. كما تتضمن تدريب الموظفين على حماية البيانات الشخصية، وإدارة حوادث تسريب البيانات عبر الإشعارات وإجراءات التعامل الفوري. بالإضافة إلى ذلك، تغطي إدارة دورة حياة البيانات، بما في ذلك الإشعارات بإدارة الموافقة، وتقييم مخاطر الحماية، وضمان حقوق أصحاب البيانات، مع مراقبة وتدقيق الامتثال. كما تتناول إدارة السجلات ذات الصلة لضمان حماية البيانات وفق أعلى المعايير.

٢/ المراجع التكميلية.

لا يوجد مراجع تكميلية .

٣/ المصطلحات والتعاريف.

١/٣ البيانات الشخصية

كل بيان - مهما كان مصدره أو شكله - من شأنه ان يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلاً للتعرف عليه بصفه مباشرة أو غير مباشرة ، ومن ذلك: الاسم، ورقم الهوية الشخصية، والعناوين، وأرقام التواصل، و أرقام الرخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي.

٤/٣ بيانات غير معالجة

البيانات التي لم تخضع للمعالجة أو للتبادل بصورة أولية بأي صيغة كانت

٥/٣ المكتب

مكتب إدارة البيانات الوطنية

٦/٣ لجنة حوكمة البيانات

هي لجنة داخلية تشكل بالجهة وهدفها مشاركة اصحاب القرار بأهمية إدارة البيانات وحماية البيانات الشخصية ونشر التوعية بالجهة

٧/٣ النظام

نظام حماية البيانات الشخصية

٨/٣ اللوائح

اللوائح التنفيذية للنظام الصادرة من الهيئة السعودية للبيانات و الذكاء الاصطناعي

٩/٣ المعالجة

أي عملية تُجرى على البيانات الشخصية بأي وسيلة كانت يدوية أو آلية، ومن ذلك: عمليات الجمع والتسجيل والحفظ والفهرسة و الترتيب و التنسيق والتخزين و التعديل و التحديث و الدمج و الاسترجاع و الاستعمال و الافصاح و النقل و النشر و المشاركة في البيانات و الربط البيئي و الحجب و المسح و الإتلاف.

١٠/٣ الجهة المختصة

الجهة التي يصدر بتحديد لها قرار من مجلس الوزراء.

٤ التخطيط

في إطار ضبط التخطيط، على الجهة أن تجري تقييمًا مبدئيًا لحماية البيانات الشخصية وتضع خطة لحماية البيانات الشخصية من أجل تلبية المتطلبات التشغيلية والاستراتيجية.

١/٤ التقييم المبدئي لحماية البيانات الشخصية

على الجهة أن تجري تقييمًا مبدئيًا لحماية البيانات الشخصية لتقييم بيئة حماية البيانات الشخصية القائمة. وينبغي للتقييم أن يشمل الآتي كحدٍ أدنى:

١. تحديد أنواع البيانات الشخصية المجمعة
٢. موقع وطريقة تخزين البيانات الشخصية
٣. المعالجة والاستخدامات الحالية للبيانات الشخصية
٤. تحديات حماية البيانات الشخصية أمام الالتزام بنظام حماية البيانات الشخصية و لوائحه التنفيذية الصادرة من الهيئة السعودية للبيانات و الذكاء الاصطناعي.

٢/٤ خطة حماية البيانات الشخصية

- بناءً على استراتيجية وخطة إدارة البيانات وحوكمتها وحماية البيانات الشخصية الخاصة بالجهة ، على الجهة أن تضع خطة لحماية البيانات الشخصية تلبى متطلبات حماية البيانات الشخصية التشغيلية والاستراتيجية وفقاً لنظام حماية البيانات الشخصية و لوائحه التنفيذية الصادرة من الهيئة السعودية للبيانات و الذكاء الاصطناعي . وعلى الخطة أن تشمل ما يلي كحدٍ أدنى:
١. خارطة طريق بالنشاطات والأهداف المرحلية لتحقيق والحفاظ على الامتثال الكامل لنظام حماية البيانات الشخصية. وعلى النشاطات أن تشمل، كحدٍ أدنى، ما يلزم لتحقيق مواصفات هذا المجال
 ٢. تخصيص الموارد والميزانية المطلوبة لتحقيق الامتثال الكامل للنظام و لوائحه التنفيذية.

٥ التدريب والتوعية

في إطار ضبط التدريب والتوعية، على الجهة أن تجري تدريبات على حماية البيانات الشخصية لغرس ثقافة متمحورة حول حماية البيانات الشخصية.

١/٥ التدريب على حماية البيانات الشخصية

على الجهة أن تجري تدريباً على حماية البيانات الشخصية لكل الموظفين من أجل غرس ثقافة تتمحور حول حماية البيانات الشخصية وفقاً لنظام حماية البيانات الشخصية و لوائحه التنفيذية الصادرة من الهيئة السعودية للبيانات و الذكاء الاصطناعي وعلى التدريب أن يشمل التالي كحدٍ أدنى:

١. أهمية حماية البيانات الشخصية وتأثيراتها وعواقبها على الجهة و/أو صاحب البيانات
٢. تعريف البيانات الشخصية
٣. حقوق صاحب البيانات
٤. مسؤوليات الجهة وصاحب البيانات
٥. الإشعارات: متى يجب إشعار الجهة أو صاحب البيانات، وكيفية التعامل مع طلبات جمع البيانات الشخصية ومعالجتها ومشاركتها

٦ تسريب البيانات

في إطار ضبط تسريب البيانات، على الجهة أن تؤسس آلية للتعامل مع تسريب البيانات.

١/٦ الإشعار بتسريب البيانات

على الجهة إشعار الجهة المختصة في حال تسريب البيانات الشخصية بما نصت عليه المادة الرابعة و العشرون من اللائحة التنفيذية التي نصت " تشعر جهة التحكم الجهة المختصة في حالة وقوع حادثة تسرب للبيانات الشخصية خلال مدة لا تتجاوز (٧٢) ساعة من وقت علمها بالحادثة، إذا كان من شأن تلك الحادثة الإضرار بالبيانات الشخصية أو صاحب البيانات الشخصية أو كانت تتعارض مع حقوقه أو مصالحه" يُرجى الرجوع إلى نظام حماية البيانات الشخصية و لوائحه التنفيذية الصادرة من الهيئة السعودية للبيانات و الذكاء الاصطناعي للاطلاع على مزيد من المتطلبات المفصلة.

٢/٦ إدارة التعامل مع تسريب البيانات

على الجهة أن ترسي وتوثق عملية إدارة التعامل مع تسريب البيانات من أجل الإدارة الفورية والمعالجة لانتهاكات حماية البيانات الشخصية ولتحديد وظائف ومسؤوليات فريق العمل المعني، وأن يتم إبلاغ السلطة التنظيمية فور المعرفة بحدوث تسريب البيانات. وعلى عملية إدارة التعامل مع التسريب أن تشمل ما يلي كحد أدنى:

١. إجراء مراجعة للحادثة من جانب ضابط حماية البيانات مع الجهة التنظيمية
٢. صياغة استجابة فورية للحادثة من جانب مسؤول ضبط البيانات و/أو معالج البيانات
٣. تنفيذ الإجراء الإصلاحي الدائم المعد من الجهة التنظيمية
٤. إجراء اختبارات على الإجراءات التصحيحية للتحقق من كفاءة حلول حماية البيانات الشخصية

يُرجى الرجوع إلى سياسة حماية البيانات الشخصية الصادرة عن مكتب إدارة البيانات الوطنية بالإضافة إلى توجيهات الهيئة الوطنية للأمن السيبراني للاطلاع على مزيد من المتطلبات المفصلة.

٧ إدارة دورة حياة البيانات

في إطار ضبط إدارة دورة الحياة، على الجهة أن تضع إطارًا للإشعار بحماية البيانات الشخصية وإدارة الموافقة وعمليات حقوق صاحب البيانات، وأن تجري عمليات تدقيق داخلية.

١/٧ الإشعارات بحماية البيانات الشخصية وإدارة الموافقة

على الجهة أن تراعي كل ما ورد في نظام حماية البيانات الشخصية ولوائحه التنفيذية لاشعار و توثيق موافقة صاحب هذه البيانات الشخصية لمعالجة بياناته.

ولمزيد من التفاصيل الرجوع إلى نظام حماية البيانات الشخصية ولوائحه التنفيذية للاطلاع .

٢/٧ حقوق صاحب البيانات

على الجهة أن ترسي وتوثق عملياتها لدعم حقوق أصحاب البيانات الشخصية، امثالاً لنظام حماية البيانات الشخصية و لوائحه التنفيذية ، والتي يتمتع فيها صاحب البيانات بالحقوق التالية:

١. الحق في العلم ويشمل ذلك إحاطته بالمسوغ النظامي لجمع بياناته الشخصية والغرض من جمعها.

٢. الحق في وصوله الى بياناته الشخصية المتوافرة لدى جهة التحكم، وفق الضوابط و الاجراءات التي تحددها اللوائح، ودون إخلال بما ورد في المادة (التاسعة) من النظام.

٣. الحق في طلب تصحيح بياناته الشخصية المتوافرة لدى جهة التحكم، أو إتمامها، أو تحديثها.

٤. الحق في طلب إتلاف بياناته الشخصية المتوافرة لدى جهة التحكم مما انتهت الحاجة إليه منها، وذلك دون إخلال بما تقتضي به المادة (الثامنة عشرة) من النظام.

على الجهة أن تطلع أصحاب البيانات على حقوقهم، وتطرح وسائل لتقديم طلبات أصحاب البيانات والاستجابة لها وتعقبها.

يُرجى الرجوع إلى نظام حماية البيانات الشخصية ولوائحه التنفيذية للاطلاع على مزيد من المتطلبات المفصلة.

٢/٧ تقييم مخاطر حماية البيانات الشخصية

على الجهة أن تجري تقييمًا لمخاطر تشغيل واستخدام أنظمة المعلومات التي تحتوي معلومات شخصية، وذلك بما يتواءم مع المادة الرابعة والعشرون (الإشعار عن حوادث تسرب البيانات الشخصية) و المادة الخامسة والعشرون (تقويم الأثر) من اللائحة التنفيذية لنظام حماية البيانات الشخصية الصادرة من الهيئة السعودية للبيانات و الذكاء الاصطناعي.

٣/٧ مراقبة وتدقيق الامتثال

على الجهة أن تجري تدقيقًا داخليًا لمراقبة الامتثال لنظام حماية البيانات الشخصية ولوائحه التنفيذية وتوثق نتائجه في تقرير يُرفع إلى مسؤول حماية البيانات. وفي حالات عدم الامتثال، على الجهة أن تتخذ إجراءات تصحيحية وتوثيقها في تقرير نتائج التدقيق. يُرجى الرجوع إلى نظام حماية البيانات الشخصية ولوائحه التنفيذية الصادرة من الهيئة السعودية للبيانات و الذكاء الاصطناعي للاطلاع على مزيد من المتطلبات المفصلة.

٨ السجلات

في إطار ضبط السجلات، على جهة التحكم الاحتفاظ بسجل أنشطة معالجة البيانات الشخصية كما هو منصوص عليه في المادة الثالثة و الثلاثون (سجلات أنشطة معالجة البيانات الشخصي) من اللائحة التنفيذية لنظام حماية البيانات الشخصية الصادرة من الهيئة السعودية للبيانات و الذكاء الاصطناعي.

المراجع

- National Data Management Office Personal Data Protection Regulation
- The General Data Protection Regulation (2018)
- California Consumer Privacy Act (2020)
- نظام حماية البيانات الشخصية الصادر بالمرسوم الملكي رقم (م/١٩١) و تاريخ ١٤٤٣/٢/١٩ هـ المعدل بالمرسوم الملكي رقم (م/١٤٨) و تاريخ ١٤٤٤/٩/١٠ هـ
- اللائحة التنفيذية لنظام حماية البيانات الوطنية