

قائمة المحتويات

المذكورة المفاهيمية بشأن حماية وأمن ومعالجة وحفظ البيانات الشخصية للهيئة الوطنية للمفقودين و المخفيين قسراً في لبنان..	1
الأسباب الموجبة:	1
كتاب قواعد إدارة السجلات المركزية للمفقودين و المخفيين قسراً المتضمن حماية وأمن ومعالجة وحفظ البيانات الشخصية للهيئة الوطنية للمفقودين و المخفيين قسراً في لبنان	5
المادة (1) التعاريف:	5
المادة (2): الأسس القانونية لمعالجة البيانات	8
المادة (3): الإلتزامات العامة للهيئة :	8
المادة (4) شروط الموافقة على معالجة البيانات:	8
المادة (5) الإلتزامات العامة للمتحكم:	8
المادة (4) الإلتزامات العامة للمعالج:	9
المادة (5) الإبلاغ عن انتهاك البيانات الشخصية:	10
المادة (6) تعيين مسؤول حماية البيانات: Assigning DPO	10
المادة (7) أدوار مسؤول حماية البيانات:	11
المادة (08) واجبات الهيئة تجاه مسؤول حماية البيانات:	11
المادة (09) حق الحصول على المعلومات:	11
المادة (10) حق طلب نقل البيانات الشخصية:	12
المادة (11) حق تصحيح أو محو البيانات الشخصية:	12
المادة (12) حق تقييد المعالجة:	13
المادة (13) الحق في إيقاف المعالجة:	13
المادة (14) حق المعالجة و المعالجة المؤتمتة:	14
المادة (15) التواصل مع الهيئة::	14
المادة (16) أمن معلومات البيانات الشخصية:	14
المادة (17) تقييم أثر حماية البيانات الشخصية:	15
المادة (18) تدابير السلامة:	16
المادة (19) خرق سلامة البيانات:	16

المذكرة المفاهيمية في شأن حماية البيانات الشخصية للهيئة الوطنية للمفوقين والمخفيين قسراً في لبنان وأمنها ومعالجتها وحفظها

الأسباب الموجبة:

إن وضع أطر لحماية البيانات الشخصية وحفظها ومعالجتها، إضافة إلى سن القوانين والإجراءات اللازمة لهذا الغرض، هو حاجة مستمرة وضرورية تُمكن الهيئة الوطنية للمفوقين والمخفيين قسراً (المشار إليها في ما يأتي بـ "الهيئة")، المسؤولة عن التعامل مع هذه البيانات، من تجنب التعرض لتبغات مالية وقانونية وإجرائية، فضلاً عن التأثير على سمعة الهيئة ونزاهتها

أعطى القانون رقم 2018/105 الهيئة الصلاحية لتجميع البيانات الشخصية ومعالجتها لأغراض إنسانية، بهدف الكشف عن مصير الأشخاص المفقودين.

ولما كانت المادة 36 من القانون 105/2018 نصت على أن كتاب قواعد إدارة السجلات المركزية للمفوقين والمخفيين قسراً يخضع لموافقة الهيئة، ما يستدعي تنظيم كتاب قواعد إدارة السجلات المركزية للمفوقين والمخفيين قسراً الذي يشمل حماية البيانات الشخصية للهيئة الوطنية للمفوقين والمخفيين قسراً في لبنان وأمنها ومعالجتها وحفظها.

أما على الصعيد الإجرائي، فإن أغلب قوانين حماية المعلومات الشخصية تعطي الأفراد حقوقاً تتعلق ببياناتهم الشخصية، مثل حق الحصول على معلوماتهم والحق بإلغاء البيانات. وقد يؤدي عدم تطبيق إجراءات حماية البيانات الشخصية إلى عثرات تشغيلية في الهيئة، ما يحتم على الهيئة وضع مبادئ أساسية لحماية البيانات الشخصية.

وفي هذا السياق، إن أغلب القوانين المعنية بحماية البيانات الشخصية مبنية على مبادئ تشكل الركيزة لكل ما هو متعلق بخصوصية البيانات الشخصية وحمايتها ومعالجتها. وتساهم هذه المبادئ في تهيئة البيئة الملائمة للمؤسسات لإتباعها لدى معالجة البيانات الشخصية بهدف حمايتها وهي:

- اعتماد مبدأ القانونية والإنصاف والشفافية لدى معالجة البيانات الشخصية.
- تحديد هدف معين عند معالجة البيانات، بما يقتضي جمع ومعالجة أقل قدر ممكن من المعلومات لتحقيق غاية مشروعة ومحددة.
- الحدّ من عدد البيانات المُعالَجة لتشمل أقلّ عدد من البيانات الشخصية.
- اعتماد الدقة والحرص على أن تكون البيانات محدثة، إضافة إلى تطبيق الإجراءات اللازمة لتصحيح المعلومات غير الدقيقة وتحديثها.
- الحدّ من فترة الإحتفاظ بالبيانات، إذ يجب ألا تُحفظ البيانات الشخصية لمدة تتجاوز الحاجة إليها.
- اعتماد مبدأَي النزاهة والسريّة، حيث يتعيّن على الهيئة اتخاذ إجراءات أمنية لحماية البيانات الشخصية من الضياع أو التلف أو الحذف.
- المحاسبة، حيث يجب وضع آليات وجداول لإثبات الامتثال للقوانين المرعية الإجراء.

مبادئ المعالجة:

في ما يتعلّق بالبيانات ذات الطابع الشخصي:

- يجب معالجتها وفقاً للقانون رقم 105 وبشكل منصف وشفاف بالنسبة لصاحب هذه البيانات.
- يجب جمعها لأهداف محدّدة وصرّوحة وألاّ تتمّ معالجتها بطريقة تتنافى مع أهداف الهيئة ومبادئها أو القانون 105. ولا تُعدّ المعالجة لأغراض الأرشفة من قبل الهيئة أو لصالحها، أو لأغراض البحث العلمي أو التاريخي أو الإحصائي، متعارضة مع الأهداف المعلنة.
- يمكن حفظها طالما كان ذلك ضرورياً لأغراض الأرشفة من قبل الهيئة، أو لأغراض علمية أو تاريخية أو إحصائية، شرط اتخاذ التدابير التقنية والتنظيمية المطلوبة بموجب القانون رقم 2018/105 لحماية حقوق أصحاب البيانات.
- يجب معالجتها بطريقة تضمن سلامتها، بما في ذلك الحماية من المعالجة غير المشروعة أو غير القانونية ومن الخرق والفقدان والتلف والأضرار، وذلك من خلال اتخاذ التدابير التقنية والتنظيمية المناسبة.

على الهيئة، بصفتها الجهة المتحكمة في البيانات الشخصية، الالتزام بشروط معيّنة. وتُعدّ الهيئة الجهة المخوّلة بتحديد غرض معالجة البيانات ووسائلها.

بما أن الهيئة هي الجهة المخوّلة بالتحكم بالبيانات، فهذا يعني تحمّلها المسؤولية لנاحية الإمتثال لجهتها و لجهة "معالج البيانات". وتشمل هذه المسؤولية الإمتثال بالآتي:

- مبادئ حماية البيانات.
 - حقوق المستخدمين.
 - إدارة إختراقات البيانات.
 - احترام المبادئ المنصوص عليها في القانون رقم 105.
 - التعامل مع معالجي بيانات مخولين ومقدّمي الضمانات الأساسية لحماية البيانات.
- لدى التعامل مع البيانات الشخصية، من المهم الإلتزام بأهمّ وأول مبدأ وهو معالجة كلّ البيانات الشخصية بطريقة قانونية عادلة مع مراعاة البعد الإنساني والأحكام القانونية ذات صلة. من هذا المنطلق، على الهيئة تطبيق/استيفاء شرط واحد على الأقل من هذه الشروط لمعالجة البيانات:

- الحصول على موافقة الفرد/المستخدم لمعالجة البيانات الشخصية.
- إهتمام (حاجة) شرعية/مبررة: من الضروري وجود حاجة مبررة لإشراك أطراف ثالثة.
- ضرورة تعاقدية: معالجة البيانات ضرورية أو شرطية للتمكن من إبرام عقد أو تنفيذه.
- موجبات قانونية : الهيئة مجبرة على معالجة البيانات الشخصية بموجب القانون رقم 105 ، مع مراعاة البعد الإنساني والأحكام القانونية ذات صلة،

- حاجة ضرورية/ملحة: معالجة البيانات الشخصية أساسية للحفاظ على حياة الأفراد/المستخدمين أو حمايتهم.
- مصلحة عامة بموجب القانون رقم 105: هذا الشرط يحقّ حصراً للسلطات الرسمية التي تمارس حقاً عاماً، أو التي تؤدي مهمات للمصلحة العامة.
- تتم معالجة البيانات الحساسة فقط بموافقة الفرد/المستخدم الصريحة، أو بما يتوافق مع المادة 2.2. بالإضافة إلى ذلك، يجوز معالجة البيانات الحساسة إذا كانت مطلوبة لرفع دعوى قانونية أو مطالبة وفقاً للفصل السادس من القانون رقم 105 (الأحكام العقابية).

في هذا السياق، على الهيئة تطبيق الخطوات العشر الآتية لتطبيق برنامج حماية البيانات الشخصية:

- 1- تعيين مسؤول عن حماية البيانات: قدمت عدة قوانين لحماية البيانات مبدأ "مسؤول حماية البيانات" وهو منصب هدفه الإشراف على برنامج الهيئة لحماية البيانات والتأكد من الإمتثال للقوانين المرعية الإجراء. بإمكان تكليف وظيفة "مسؤول حماية البيانات" لموظف موجود مسبقاً بالهيئة أو إعطاء هذه الوظيفة لموظف جديد. على "مسؤول حماية البيانات" أن يكون مستقلاً، خبيراً في أمن البيانات وحمايتها، ملماً بهذا المجال، ويقدم التقرير إلى أعلى المستويات الإدارية. وعلى مسؤول حماية البيانات المساعدة في مراقبة الإمتثال الداخلي مع قوانين حماية البيانات المرعية الإجراء، وتقديم المشورة للهيئة على موجباتها لحماية البيانات، والعمل كجهة اتصال للأفراد وهيئات حماية البيانات.
- 2- الحفاظ على سجل البيانات الشخصية: من أجل حفظ البيانات الشخصية، على الهيئة معرفة البيانات التي تجمعها، كيفية استخدامها، وكيفية حفظها. ويتم ذلك من خلال معرفة كل العمليات المعتمدة في الهيئة التي تتضمن البيانات الشخصية، وتوثيقها، وكيفية استعمالها وأسبابها، إضافة إلى مكان ومدة حفظها ضمن "سجل البيانات الشخصية". وعلى السجل أن يتضمن:
 - إسم ومعلومات التواصل مع "مسؤول حماية البيانات" و أي طرف ثالث.
 - الأسس المشروعة والهدف من معالجة البيانات.
 - الفئات المختلفة من البيانات المعالجة.
 - الأنظمة وأماكن معالجة البيانات الشخصية.
 - أماكن نقل البيانات ولائحة المتلقين.
 - فترة حفظ البيانات والإجراءات التقنية والأمنية الملزمة.
- 3- إرسال إشعار بالهدف والحصول على الموافقة: بما أن الشفافية هي ركيزة أساسية في قوانين معالجة البيانات الشخصية.
- 4- الإستجابة عند طلب/استفسار الأفراد عن بياناتهم الشخصية.
- 5- تطبيق و فرض آليات أمنية.

- 6- تضمين خصوصية البيانات ضمن النظام، والإجراءات، والخدمات.
 - 7- إرسال إشعار عند حصول خرق للبيانات.
 - 8- إدارة الأطراف الثالثة.
 - 9- حماية البيانات الشخصية عند نقلها لخارج الحدود.
 - 10- نشر سياسات، وإجراءات، وممارسات حماية البيانات لدى الهيئة.
-

كتاب قواعد إدارة السجلات المركزية للمفقودين والمخفيين قسراً
المتّمل بحماية البيانات بما فيها الشخصية
لدى الهيئة الوطنية للمفقودين والمخفيين قسراً في لبنان وأمنها ومعالجتها وحفظها
تُعدّ هذه الأنظمة الداخلية وثيقة عامة، ومتاحة على الموقع الإلكتروني للهيئة.

المادة (1) التعاريف:

الهيئة: الهيئة الوطنية المقررة والمعترف عنها بالقانون رقم 105/2018، وهي المسؤولة الوحيدة عن تطبيق هذا الكتاب والتعيينات كافة.

نطاق التطبيق:

- 1- تطبق الأحكام الواردة في هذا الكتاب على كلّ المعالجات الآلية وغير الآلية للبيانات ذات الطابع الشخصي العائدة للمفقودين والمخفيين قسراً في لبنان من قبل الهيئة
- 2- تُطبّق الأحكام المنصوص عليها في هذه الوثيقة عند إجراء المعالجة داخل لبنان

البيانات عامة وفئاتها:

ينحصر تعريف البيانات بالمفقودين والمخفيين قسراً، إضافة إلى الرفات بحسب القانون 105/2018.

- البيانات: مجموعة منظمة أو غير منظمة من المعطيات حول المفقودين أو المخفيين قسراً أو الوقائع أو المفاهيم أو التعليمات أو المشاهدات أو القياسات التي تكون على شكل أرقام أو حروف أو كلمات أو رموز أو صور أو فيديو أو إشارات أو أصوات أو خرائط أو أي شكل آخر، يتم تفسيرها أو تبادلها أو معالجتها، عن طريق الأفراد أو الحواسيب، وتشمل المعلومات أينما وردت في هذا الكتاب مع مراعاة المادة الرابعة (السرية) من النظام الداخلي العائدة للهيئة.
- البيانات الشخصية: أي بيانات تتعلق بالمفقودين أو المخفيين قسراً والتي تمكّن من التعرف على صاحب البيانات بشكل مباشر أو غير مباشر من خلال الربط بين البيانات، واستخدام عناصر التعريف كإسمه، أو صوته، أو رقمه التعريفي، أو المعرف الإلكتروني الخاص به، أو موقعه الجغرافي، أو صفة أو أكثر من صفاته الشكلية أو الفيزيولوجية، أو الإقتصادية، أو الثقافية أو الإجتماعية وتشمل البيانات الشخصية الحساسة و البيانات الحيوية البيومترية.
- البيانات الشخصية الحساسة: أي بيانات تكشف بشكل مباشر أو غير مباشر عن عائلة، أو تدور حول المفقودين أو المخفيين قسراً أو صاحب البيانات، وأصله العرقي أو أرائه السياسية أو الفلسفية أو معتقداته الدينية، أو سجل السوابق الجنائية الخاص به أو بيانات القياسات الحيوية البيومترية الخاصة به، أو أي بيانات تتعلق بصحة هذا الشخص وتشمل حالته الجسدية أو النفسية أو الذهنية أو العقلية أو البدنية أو الجينية أو الجنسية، الرفات، بما في ذلك المتعلقة بمقدّم خدمات الرعاية الصحية والإجتماعية له التي تكشف عن وضعه الصحي، و المقابر الجماعية.
- "البيانات البيومترية": هي البيانات ذات الطابع الشخصي الناتجة عن معالجة تقنية محدّدة تتعلق بالخصائص الجسدية أو الفيزيولوجية أو السلوكية للشخص الطبيعي، والتي تسمح بتحديد أو تأكيد الهوية الفريدة لهذا الشخص الطبيعي، مثل صور الوجه أو البصمة أو بيانات dactyloscopic، وغيرها.
- صاحب البيانات: الشخص الطبيعي، موضوع البيانات الشخصية.

- "المسؤول عن معالجة البيانات ذات الطابع الشخصي" (أو المسؤول عن المعالجة): داخل الهيئة، الشخص الذي يُبلغ ويُقدّم المشورة أو التوصيات إلى لجنة البيانات هو موظف حماية البيانات (DPO). يُقدّم موظف حماية البيانات المشورة بشأن ما إذا كان يجب إجراء تقييم لأثر حماية البيانات أم لا. كما يقوم بجمع المعلومات لتحديد أنشطة المعالجة، ويحلّل ويتحقّق من مدى امتثال أنشطة المعالجة للقانون المعمول به. ولا يتحمّل موظف حماية البيانات مسؤولية الإمتثال، إذ تقع هذه المسؤولية على عاتق الهيئة.
- "المرسل إليه البيانات ذات الطابع الشخصي" : هو الشخص المخوّل بتلقي البيانات الشخصية، والذي يختلف عن صاحب البيانات الشخصية أو موظف حماية البيانات (DPO) أو الهيئة
- المتحكم : controller الهيئة هي المتحكم بالبيانات الشخصية. إضافة إلى ذلك، قد تكون هناك جهات أخرى مشتركة في التحكم في البيانات.
- المعالج : processor شخص طبيعي أو جهة تقوم بمعالجة البيانات الشخصية نيابةً عن الهيئة أو وفقاً لتوجيهات وتعليمات الهيئة.
- المعالجة: تعني أية عملية، أو مجموعة من العمليات، سواء كانت آلية أو غير آلية، يتمّ إجراؤها على البيانات الشخصية، بما في ذلك على سبيل المثال لا الحصر، جمع أو تسجيل أو تنظيم أو هيكلة أو تخزين أو تكييف أو تغيير أو استرجاع أو استشارة أو استخدام أو نقل (سواء في شكل إلكتروني أو شفهي أو خطياً) أو النشر أو الإتاحة أو التصحيح أو التلف؛ يكون لمصطلحي "عملية" و"معالجة" معاني مترابطة.
- آلية إخفاء الهوية : ID Masking آلية إخفاء الهوية هي عبر المعالجة التي يتمّ إجراؤها على البيانات الشخصية بطريقة تخفي هوية صاحب البيانات ولا تربط هذه البيانات به أو تنسبها له ولا تتيح إمكانية التعرف عليه بأية طريقة كانت.
- المعالجة الآلية : المعالجة التي تتم باستخدام برنامج أو نظام إلكتروني يعمل بطريقة آلية وتلقائية إما بشكل مستقل كلياً من دون أي تدخل بشري أو بشكل جزئي بإشراف و تدخل بشري محدود.
- أمن البيانات الشخصية : مجموعة من التدابير والإجراءات والعمليات التقنية والتنظيمية المحددة وفقاً لهذا الكتاب التي من شأنها الحفاظ على حماية الخصوصية وسريّة وسلامة ووحدة البيانات الشخصية وتكاملها وتوافرها.
- آلية إخفاء البيانات : المعالجة التي يتمّ إجراؤها على البيانات الشخصية بطريقة تؤدي بعد إتمام المعالجة إلى عدم إمكانية ربط وتنسب هذه البيانات بصاحب البيانات من دون استخدام معلومات إضافية، شرط أن تكون تلك المعلومات الإضافية محفوظة بشكل مستقل وآمن، ووفقاً للتدابير والإجراءات التقنية والتنظيمية المحددة بموجب أحكام هذا الكتاب، لضمان عدم إرباط البيانات الشخصية بشخص طبيعي محدّد أو يمكن التعرف عليه من خلالها.
- خرق وانتهاك البيانات : يعني خرقاً أمنياً يؤدي إلى التدمير أو الفقدان أو التعديل العرضي أو غير المشروع للبيانات الشخصية، أو الكشف غير المصرح به عنها، أو الوصول غير المصرح به إليها، سواء تم نقلها أو تخزينها أو معالجتها بأية طريقة أخرى.
- التنميط (Profiling) : شكل من أشكال المعالجة الآلية بحيث تتضمن استخدام البيانات الشخصية لتقييم جوانب شخصية معينة ومرتبطة بصاحب البيانات، ومن بينها تحليل أو توقع الجوانب المتعلقة بأدائه أو وضعه المالي أو صحته أو تفضيلاته الشخصية أو إهتماماته أو سلوكه أو مكانه أو تحركاته أو موثوقيته.

- المعالجة عبر الحدود: نشر أو استخدام أو عرض أو إرسال أو استقبال أو استرجاع أو استخدام أو مشاركة البيانات الشخصية أو معالجتها خارج النطاق الجغرافي للدولة.
- الموافقة: تعني أي تعبير عن الإرادة يتم بحرية، ويكون محدداً ومبنياً على علم، يقدمه صاحب البيانات للدلالة على موافقته على معالجة البيانات الشخصية المتعلقة به.

في حال كانت المعالجة تستند إلى موافقة صاحب البيانات الشخصية، يجب استيفاء الشروط الآتية:

- يجب على الهيئة أن تكون قادرة على إثبات أنها حصلت على موافقة صاحب البيانات لمعالجة بياناته.
- يجب إبلاغ صاحب البيانات الشخصية بأنه يمكنه سحب موافقته في أي وقت، من دون أن يؤثر ذلك على قانونية المعالجة التي تمت قبل تاريخ السحب، والتي تظل خاضعة لأحكام هذه الوثيقة. ويجب على وجه الخصوص إبلاغ صاحب البيانات بالحالات التي يجوز فيها للهيئة تجاوز رفضه، مثلاً: نقل بياناته إلى أطراف ثالثة وفقاً للمادة 2.2، أو الاستثناءات من حقه في تصحيح أو حذف البيانات الشخصية بموجب المادة 11، أو الاستثناءات من حقه في تقييد المعالجة بموجب المادة 12، أو الاستثناء من حقه في الاعتراض على المعالجة والمعالجة الآلية لبياناته بموجب المادة 14). ويجب تزويد صاحب البيانات بإشعار معلوماتي بهذا الخصوص.

المادة 2: الأسس القانونية لمعالجة البيانات

2.1.1. المبدأ

تتولى الهيئة، بموجب القانون رقم 105، العمل لأغراض إنسانية بحتة، وتحديدًا للكشف عن مصير ومكان وجود المفقودين والمخفيين قسراً.

يشمل عمل الهيئة قضايا المفقودين والمخفيين قسراً، ما يمكن الهيئة من التحكم في البيانات ومعالجتها وفقاً للشروط التالية. وبناءً عليه، تشمل الأسس القانونية لمعالجة البيانات الشخصية من قبل الهيئة بموجب القانون رقم 105 ما يأتي:

- يجب أن تكون المعالجة ضرورية لحماية المصلحة العامة، وبشكل خاص للكشف عن مصير المفقودين والمخفيين قسراً.
- يجب أن تكون المعالجة ضرورية لأغراض الأرشفة، أو لأغراض الدراسات العلمية أو التاريخية أو الإحصائية، وفقاً لأنظمة الهيئة وتعليماتها.
- يجب أن تكون المعالجة ضرورية للوفاء بالتزامات الهيئة كما هو محدد في القانون رقم 105.
- أن تكون الهيئة قد حصلت على موافقة صاحب البيانات وسجلتها.

2.2. الحالة الخاصة بنقل البيانات إلى طرف ثالث بما في ذلك دولة أجنبية أو منظمة دولية

2.2.1 يسمح بنقل البيانات ذات الطابع الشخصي إلى طرف ثالث في حال كانت الهيئة تعتبر بموجب القرارات الصادرة عنها أن هذه الدولة أو المنظمة تضمن مستوى كافٍ من الحماية لهذه البيانات بموجب القوانين والأنظمة السارية على مستلم البيانات ذات الطابع الشخصي

2.2.2 من حيث المبدأ، يجب على الهيئة أن تستحصل على موافقة صاحب البيانات وتسجلها قبل نقل أي من بياناته إلى طرف ثالث ويجب أن يكون الهدف من النقل إنسانياً بحت.

2.2.3 واستثناءياً، وفي حال كان الغرض من النقل هو توضيح مصير ومكان وجود الأشخاص المفقودين وفقاً للقانون رقم 105، يجوز للهيئة نقل البيانات الشخصية إذا لم يوافق صاحب البيانات على ذلك أو في حال إستحالة الوصول إليه ، وذلك وفقاً للشروط الآتية مجتمعة:

1. أن تقوم الهيئة بمراجعة الحالة لتقييم أسباب رفض صاحب البيانات،
2. أن تُجري الهيئة تقييماً للمخاطر للتأكد من أن النقل لا يشكل خطراً على صاحب البيانات،
3. أن تكون الهيئة وقعت اتفاقية مع الطرف الثالث لتوضيح الشروط التي يمكن بموجبها استخدام البيانات المنقولة، وضمن أمن البيانات بعد نقلها،
4. أن يكون الغرض الوحيد من نقل البيانات الشخصية من قبل الهيئة هو توضيح مصير الأشخاص المفقودين ومكان وجودهم،
5. أن تكون الهيئة قد أبلغت صاحب البيانات بأنها ستنتقل بياناته رغم رفضه، وذلك قبل تنفيذ عملية النقل

المادة (3) الإلتزامات العامة للهيئة:

يجب على الهيئة الإلتزام بما يأتي:

- اتخاذ الإجراءات والتدابير التقنية والتنظيمية الملائمة لتطبيق المعايير القياسية اللازمة لحماية و تأمين البيانات الشخصية حفاظاً على سريتها وخصوصيتها، و ضمان عدم اختراقها أو إتلافها أو تغييرها أو العبث بها، مع مراعاة طبيعة ونطاق وأغراض المعالجة واحتمالية وجود مخاطر على سريّة وخصوصية البيانات الشخصية لصاحب البيانات.
- تطبيق التدابير الملائمة سواء أثناء تحديد وسائل المعالجة أو أثناء المعالجة نفسها وذلك بهدف الإمتثال لأحكام هذا الكتاب والضوابط المنصوص عليها في "تدابير آلية إخفاء البيانات".
- تطبيق التدابير التقنية والتنظيمية الملائمة بالنسبة للإعدادات التلقائية، للتأكد من اقتصار معالجة البيانات الشخصية على الغرض المحدد لها. و يطبق هذا الإلتزام على حجم ونوع البيانات الشخصية التي يتم جمعها، و نوع المعالجة التي سيتم اجراءها عليها وفترة تخزين هذه البيانات، ومدى إمكانية الوصول اليها.
- مسك سجل الكتروني خاص للبيانات الشخصية على أن يتضمن هذا السجل بيانات كل من الهيئة ومسؤول حماية البيانات وبيان وصف فئات البيانات الشخصية لديه، وبيانات الأشخاص المصرح لهم بالوصول إلى البيانات الشخصية، والمدة الزمنية للمعالجة وقيودها ونطاقها، وآلية محو البيانات الشخصية أو تعديلها أو معالجتها لديه، والغرض من المعالجة، وأي بيانات متعلقة بحركة ومعالجة تلك البيانات عبر الحدود، وبيان الإجراءات التقنية والتنظيمية الخاصة بأمن المعلومات وعمليات المعالجة، على أن تقوم الهيئة بتوفير هذا السجل للهيئة متى ما طلب منه ذلك.
- أي التزامات أخرى يتم تحديدها بناءً على تطور وسير أعمال الهيئة.

المادة (4) الالتزامات العامة لمقدمي الخدمات:

عند التعاقد مع معالجين، يجب على الهيئة التأكد من أنها تملك الضمانات الكافية لتنفيذ التدابير الفنية والتنظيمية التي تضمن أن عملية المعالجة تفي بالمطلوبات والقواعد والأنظمة الخاصة بالمعالجة.

يجب على المعالج الالتزام بما يأتي:

- إجراء المعالجة وتنفيذها وفقا لتعليمات الهيئة، والعقود والاتفاقات المبرمة بينهم التي تحدّد على وجه الخصوص نطاق المعالجة وموضوعها وغرضها وطبيعتها ونوع البيانات الشخصية وفئات أصحاب البيانات.
- تطبيق الإجراءات والتدابير التقنية والتنظيمية الملائمة لحماية البيانات الشخصية في مرحلة التصميم، سواء أثناء تحديد وسائل المعالجة أو أثناء المعالجة نفسها على أن يراعى فيها تكلفة تطبيق هذه الإجراءات والتدابير وطبيعة المعالجة ونطاقها وأغراضها.
- إجراء المعالجة وفق الغرض و المدة المحددة لها، و في حال تجاوزت المعالجة المدة المحددة يجب عليه أن يخطر للهيئة بذلك ليأذن له بتمديد هذه المدة أو يصدر إليه التوجيهات المناسبة.
- محو البيانات بعد انقضاء مدة المعالجة أو تسليمها للهيئة.
- حماية وتأمين عملية المعالجة وتأمين الوسائط والأجهزة الإلكترونية المستخدمة في المعالجة وما عليها من بيانات شخصية.
- مسك سجل خاص للبيانات الشخصية التي تتم معالجتها نيابة عن الهيئة.
- على أن يتضمن هذا السجل بيانات كل من الهيئة والمعالج ومسؤول حماية البيانات وبيان وصف فئات البيانات الشخصية لديه، وبيانات الأشخاص المصرح لهم بالوصول إلى البيانات الشخصية، والمدة الزمنية للمعالجة وقيودها ونطاقها، وآلية محو البيانات الشخصية أو تعديلها أو معالجتها لديه، والغرض من المعالجة، وأي بيانات متعلقة بحركة ومعالجة تلك البيانات عبر الحدود، وبيان الإجراءات التقنية والتنظيمية الخاصة بأمن المعلومات وعمليات المعالجة على أن يقوم المعالج بتوفير هذا السجل للهيئة متى ما طلب منه ذلك.
- توفير كافة الوسائل لإثبات التزامها بتطبيق أحكام هذا الكتاب/النظام عند طلب الهيئة ذلك.
- إجراء المعالجة وتنفيذها طبقا للقواعد والشروط والضوابط المحددة بهذا الكتاب ولائحته التنفيذية أو التي يصدر بموجبها تعليمات من الهيئة.
- تُنفذ المعالجة بموجب عقد أو اتفاق خطي يحدّد بوضوح التزامات مقدمي الخدمات وواجباتهم وأدوارهم في عملية المعالجة.

المادة (5) الإبلاغ عن انتهاك البيانات الشخصية:

- يجب على الهيئة، بدعم من موظف حماية البيانات (DPO)، أن تعالج على الفور أي خرق للبيانات الشخصية. ويجب على الهيئة إصدار تقرير يتضمن ما يأتي:
- 1- بيان طبيعة الاختراق أو الانتهاك، وصورته، وأسبابه، والعدد التقريبي له و سجلاته.
- 2- بيانات مسؤول حماية البيانات المعني لديها.
- 3- الآثار المحتملة والمتوقعة لحدوث هذا الاختراق أو الانتهاك.

4- بيان الإجراءات والتدابير المتخذة من قبله والمقترح تنفيذها لمواجهة هذا الاختراق أو الانتهاك والتقليل من آثاره السلبية.

5- توثيق الاختراق أو الانتهاك والإجراءات التصحيحية المتخذة من قبله.

6- أي توصيات أخرى.

- في كل الحالات، يجب على الهيئة إبلاغ صاحب البيانات عند حدوث خرق أو انتهاك يلحق ضرراً بخصوصية بياناته الشخصية أو سريتها أو أمنها، وذلك في أقرب وقت ممكن. كما يجب على الهيئة إعلام صاحب البيانات بالإجراءات التي تم اتخاذها في هذا الشأن.

المادة (6) تعيين مسؤول حماية البيانات. Assigning DPO :

- يجب على الهيئة تعيين مسؤول لحماية البيانات تتوفر لديه الكفاءات المتعلقة بحماية البيانات الشخصية، وذلك في أي من الحالات الآتية:
- 1- إذا كانت المعالجة من شأنها إحداث خطر ذي مستوى عالي على سرية وخصوصية البيانات الشخصية لصاحب البيانات نتيجة اعتماد تقنيات جديدة أو مرتبطة بحجم البيانات.
- 2- إذا كانت المعالجة ستتضمن تقييماً ممنهجاً وشاملاً للبيانات الشخصية الحساسة بما يشمل التنميط والمعالجة الآلية.
- 3- إذا كانت المعالجة ستتضمن على حجم كبير من البيانات الشخصية الحساسة.
- 4- في حال اقتضى الأمر إجراء تقييم لأثر حماية البيانات.
- يجوز أن يكون مسؤول حماية البيانات موظفاً لدى الهيئة أو مخول من قبلها سواء بموجب كتاب قواعد البيانات أو خارجها أو بأي وسيلة أخرى.
- على الهيئة تحديد عنوان الاتصال بمسؤول حماية البيانات.
- تحدّد اللائحة التنفيذية لهذا الكتاب أنواع التقنيات ومعايير تحديد حجم البيانات المطلوبة وفقاً لهذه المادة.

المادة (7) أدوار مسؤول حماية البيانات:

- يتولى مسؤول حماية البيانات التأكد من مدى امتثال الهيئة بتنفيذ أحكام هذا الكتاب ولائحته التنفيذية والتعليمات الصادرة عن الهيئة، ويتولى مسؤول حماية البيانات على وجه الخصوص القيام بالمهام والصلاحيات الآتية:
- 1- التحقق من جودة الإجراءات المعمول بها لدى الهيئة وصحتها.
- 2- تلقي الطلبات والشكاوى المتعلقة بالبيانات الشخصية وفقاً لأحكام هذا الكتاب.
- 3- تقديم الاستشارات الفنية الخاصة بإجراءات التقييم والفحص الدوري لأنظمة حماية البيانات الشخصية لدى الهيئة، وأنظمة منع الاختراق، وتوثيق نتائج هذا التقييم، وتقديم التوصيات المناسبة بشأنها بما فيها إجراءات تقييم المخاطر.
- 4- العمل كنقطة ارتكاز داخل الهيئة، حسب الحالة، في ما يتعلق بتنفيذ أحكام معالجة البيانات الشخصية المنصوص عليها في هذه الوثيقة.
- 5- دعم الهيئة عند إجراء تقييم لأثر حماية البيانات.
- 6- أي مهام أو صلاحيات أخرى يتم تحديدها في هذا الكتاب.

ويجب على موظف حماية البيانات الحفاظ على سرية المعلومات والبيانات التي يتلقاها أثناء أداء مهامه وممارسة صلاحياته، وذلك وفقاً لما هو منصوص عليه في هذا الكتاب ووفقاً لقوانين الهيئة وأنظمتها.

المادة (08) واجبات الهيئة تجاه مسؤول حماية البيانات:

- على الهيئة توفير كافة السبل لضمان أداء مسؤول حماية البيانات الأدوار والمهام الموكلة إليه والمنصوص عليها في المادة (7) من هذا الكتاب بالشكل المطلوب، وعلى وجه الخصوص ما يأتي:
 - 1- ضمان إشراكه بشكل مناسب و في الوقت الملائم في كافة المسائل المتعلقة بحماية البيانات الشخصية.
 - 2- ضمان تزويده بكافة الموارد اللازمة وتقديم الدعم اللازم له لتنفيذ المهام الموكلة إليه.
 - 3- عدم إنهاء خدماته أو فرض أي جزاء تأديبي بسبب يتعلق بتأديته لمهامه وفقاً لأحكام هذا الكتاب.
 - 4- ضمان عدم تكليفه بمهام تؤدي إلى تعارض في المصالح بينها وبين المهام المحددة له وفقاً لهذا الكتاب.
- يمكن لصاحب البيانات التواصل مباشرة مع الهيئة ووفقاً للأصول المعتمدة لديها بكل ما يتعلق ببياناته الشخصية ومعالجتها لتمكينه من ممارسة حقوقه وفقاً لأحكام هذا الكتاب.

المادة (09) حق الحصول على المعلومات:

- يحق لصاحب البيانات وبناء على طلب خطي يقدمه للهيئة، ووفقاً للأصول العائدة لها ومن دون أي مقابل الحصول على المعلومات الآتية:
- 1- أنواع البيانات الشخصية التابعة له التي تتم معالجتها.
- 2- أغراض المعالجة.
- 3- القرارات المتخذة بناء على المعالجة الآلية، بما فيها التمييز.
- 4- القطاعات أو المنشآت المستهدفة التي ستتم مشاركة بياناته الشخصية معها من داخل وخارج الحدود.
- 5- الضوابط والمعايير المتعلقة بفترات تخزين البيانات الشخصية وصيانتها.
- 6- إجراءات تصحيح المعالجة أو إلغائها أو تقييدها والإعراض على بياناته الشخصية.
- 7- تدابير الحماية الخاصة بالمعالجة عبر الحدود التي تتم وفقاً للمادة (22) من هذا الكتاب.
- 8- الإجراءات التي ستتخذ في حال اختراق أو انتهاك بياناته الشخصية، خصوصاً إذا كان الاختراق أو الانتهاك له خطر مباشر وجسيم على خصوصية بياناته الشخصية وسريتها.
- 9- كيفية تقديم الطلب للهيئة.

في كل الحالات، يجب على الهيئة، قبل البدء في المعالجة، تزويد صاحب البيانات بالمعلومات المنصوص عليها في البنود 1/ و 2/ و 4/ و 7/ من الفقرة 1/ من هذه المادة.

يجوز للهيئة رفض طلب صاحب البيانات بالوصول إلى المعلومات المذكورة في الفقرة 1/ من هذه المادة، إذا ثبت لديها ما يأتي:

- 1- أن الطلب لا يتعلق بالمعلومات الواردة في الفقرة 1/ من هذه المادة أو يتكرر بشكل مفرط.

2- أن الطلب قد يؤثر سلباً على جهود الهيئة في حماية أمن المعلومات.

3- أن الطلب قد يؤثر سلباً على جهود الهيئة في الكشف عن مصير المفقودين والمخفيين قسراً.

4- أن الطلب يلحق ضرراً بخصوصية البيانات الشخصية لأطراف ثالثة وسريتها.

المادة (10) حق طلب نقل البيانات الشخصية:

- يحق لصاحب البيانات وبناء على طلب خطي يقدمه للهيئة، ووفقاً للأصول العائدة لها الحصول على البيانات الشخصية الخاصة به التي تم تزويدها للمتحم للمعالجتها، وذلك بشكل منظم وقابل للقراءة آلياً متى ما كانت المعالجة مبنية على موافقة صاحب البيانات، أو ضرورة لتنفيذ التزام عقدي، ومنفذة بوسائل آلية.
- يحق لصاحب البيانات طلب نقل بياناته الشخصية للهيئة آخر متى ما كان ذلك ممكناً من الناحية التقنية، وإن لا يتعارض مع جهود الهيئة في الكشف عن مصير المفقودين والمخفيين قسراً .

المادة (11) حق تصحيح أو محو البيانات الشخصية:

- يحق لصاحب البيانات وبناء على طلب خطي يقدمه للهيئة، ووفقاً للأصول العائدة لها، طلب تصحيح بياناته الشخصية غير الدقيقة، أو استكمالها لدى الهيئة من دون تأخير غير مبرر.
 - يحق لصاحب البيانات طلب محو بياناته الشخصية الخاصة لدى الهيئة في أي من الحالات الآتية:
 - 1- لم تعد بياناته الشخصية ضرورية للأغراض التي جمعت أو عولجت من أجلها.
 - 2- عدول صاحب البيانات عن الموافقة التي بنيت عليها المعالجة.
 - 3- اعتراض صاحب البيانات على المعالجة، أو غياب الأسباب المشروعة للهيئة في الاستمرار بالمعالجة.
 - 4- أن معالجة بياناته الشخصية تمت بمخالفة أحكام هذا الكتاب والتشريعات السارية، وأن عملية المحو ضرورية للإمتثال للتشريعات والمعايير المعتمدة المعمول بها في هذا الشأن.
 - باستثناء الحالات التي تكون فيها الموافقة من صاحب البيانات هي الأساس القانوني لمعالجة البيانات، يجوز للهيئة رفض حذف البيانات إذا كانت مواصلة معالجة البيانات الشخصية ضرورية للكشف عن مصير الشخص المفقود أو مكان تواجده، أو إذا كانت ضرورية لأغراض تاريخية أو إحصائية أو علمية، وذلك فقط وفقاً للشروط المنصوص عليها في
- المادة 2.2.3.

المادة (12) حق تقييد و/أو إيقاف المعالجة:

يحق لصاحب البيانات إلزام الهيئة بتقييد و/أو إيقاف المعالجة بموجب طلب خطي إلى الهيئة ليُصار إلى بحثه وذلك في أي من الحالات الآتية:

- 1- اعتراض صاحب البيانات على دقة بياناته الشخصية، و في هذه الحالة يتم تقييد المعالجة لفترة معينة تسمح للمتحم التحقق من دقتها.

- 2- إعتراض صاحب البيانات على معالجة بياناته الشخصية بالمخالفة للأغراض المتفق عليها.
 - 3- أن تكون المعالجة قد تمت بمخالفة أحكام هذا الكتاب والتشريعات السارية.
 - 4- إذا كانت المعالجة لأغراض التسويق المباشر بما في ذلك التنميط ذات العلاقة بالتسويق المباشر.
 - 5- إذا كانت المعالجة لأغراض إجراء المسح الإحصائي.
 - 6- إذا كانت المعالجة تتم بالمخالفة لمبادئ معالجة البيانات وذلك فقط وفقاً للشروط المنصوص عليها في المادة 2.2.3
 - "حالات معالجة البيانات الشخصية من دون موافقة صاحبها" من هذا الكتاب.
 - 7- إذا تبين ان المعالجة تعرّض صاحب البيانات للخطر.
- على الرغم مما ورد في هذه المادة، يجوز للهيئة المضي قدماً في معالجة البيانات الشخصية لصاحب البيانات في أي من الحالات وذلك فقط وفقاً للشروط المنصوص عليها في المادة 2.2.3:
1. إذا كانت المعالجة مقتصرة على تخزين البيانات الشخصية لأغراض تاريخية.
 2. إذا كانت المعالجة ضرورية لتحقيق المصلحة العامة وبعد إجراء تقييم للمخاطر للتأكد من أن المعالجة لا تُشكّل خطراً على صاحب البيانات.
 3. إذا كانت المعالجة ضرورية لحماية حقوق أطراف ثالثة وفقاً للتشريعات المعمول بها.
- في كلّ الحالات، يجب على الهيئة، عند رفع القيود المنصوص عليها في هذه المادة، إخطار صاحب البيانات بذلك.
- لغرض هذه المادة، يُقصد بالتقييد: وضع علامة على البيانات الشخصية المخزنة بهدف الحد من معالجتها في المستقبل؛
- لغرض هذه المادة، يُقصد بالإيقاف: التوقف عن أي عمليات تُجرى على البيانات الشخصية لمدة محددة أو غير محددة.
- المادة (13) حق المعالجة والمعالجة الآلية:**
- يحق لصاحب البيانات الاعتراض لدى الهيئة، ووفقاً للأصول المحددة لديها على القرارات التي تصدر عن المعالجة الآلية وتكون لها تبعات قانونية أو تؤثر بشكل جسيم على صاحب البيانات، بما فيها التنميط.
- على الرغم مما ورد في البند الأول من هذه المادة، لا يجوز لصاحب البيانات الاعتراض على القرارات التي تصدر عن المعالجة الآلية في الحالات الآتية:
- 1- إذا كانت المعالجة الآلية ضمن شروط التعاقد بين صاحب البيانات والهيئة.
 - 2- إذا تمت الموافقة المسبقة من صاحب البيانات على المعالجة الآلية وفق الشروط المحددة في المادة (4) "شروط الموافقة على معالجة البيانات" من هذا الكتاب.
- يجب على الهيئة تطبيق إجراءات وتدابير مناسبة لحماية خصوصية وسرية البيانات الشخصية لصاحب البيانات في الحالات المشار إليها في البند الثاني من هذه المادة، وعدم الإضرار والمساس بحقوقه.

- يتعين على الهيئة إدخال العنصر البشري في مراجعة قرارات المعالجة الآلية بناء على طلب صاحب البيانات.

المادة (14) التواصل مع الهيئة:

على الهيئة توفير طرق وآليات مناسبة وواضحة لتمكين صاحب البيانات من التواصل معها وطلب ممارسة أي من حقوقه المنصوص عليها في هذا الكتاب ووفقاً للأنظمة التنفيذية التي قد تصدر عن الهيئة.

المادة (15) أمن معلومات البيانات الشخصية:

- يجب على الهيئة وضع واتخاذ إجراءات وتدابير تقنية وتنظيمية ملائمة، لضمان تطبيق مستوى أمن المعلومات الذي يتناسب مع المخاطر المصاحبة للمعالجة وفق أفضل المعايير والممارسات الدولية، و يمكن أن يشمل ذلك الآتي:

- 1- تشفير البيانات الشخصية وتطبيق آلية إخفاء البيانات.
- 2- تطبيق إجراءات وتدابير تضمن استمرار سرية أنظمة وخدمات المعالجة، وسلامتها وصحتها ومرونتها.
- 3- تطبيق إجراءات وتدابير تضمن استرجاع البيانات الشخصية والوصول إليها في الوقت المحدد في حال حدوث أي عطل فعلي أو فني.
- 4- تطبيق إجراءات تضمن سلسلة عملية الاختبار وتقييم فاعلية التدابير التقنية والتنظيمية وتأمينها بما يضمن أمن المعالجة.
- 5- عدم اعتماد البريد الإلكتروني الخاص لنقل المعلومات.
- 6- وجوب إتمام كل التواصل عبر البريد الإلكتروني، سواء داخلي أو خارجي تحت مبدأ "الحاجة إلى المعرفة" - "need to-know basis" حيث يجب مشاركة البيانات الشخصية مع الأفراد المعنيين فقط لتجنب تفشيها.
- 7- الولوج عن بعد للخادم، واستخدام الحاسوب المنزلي أو النقل يجب أن يمتثل لمعايير السلامة الموضحة في سياسة أمن المعلومات لدى الهيئة بالبيانات.
- 8- يجب تجنب استخدام شبكات الإنترنت والاتصال اللاسلكي الغير آمن لسحب البيانات الشخصية أو تبادلها، أو نقلها، أو بثها، إلا في حالة الضرورات التشغيلية.
- 9- على الموظفين الذين يتعاملون مع البيانات الشخصية اتخاذ الحذر عند الإتصال بخادم الهيئة بالبيانات عن بعد.
- 10- على كلمات السر أن تكون آمنة ومحفوظة وعلى الموظفين التأكد من تسجيل الخروج بطريقة ملائمة وإغلاق المتصفحات.
- 11- على الأجهزة المحمولة أن تستعمل في أماكن آمنة عند العمل في ظروف صعبة أو خطيرة.
- 12- يجب تجنب استخدام الأجهزة المحمولة لحفظ البيانات الشخصية المصنفة كحساسة، وفي حال عدم توفر حل آخر، يجب نقل البيانات الشخصية الحساسة إلى قاعدة بيانات وتطبيقات حفظ بيانات ملائمة فور إمكانية ذلك.
- 13- في حال استخدام USB وبطاقات الذاكرة ومحركات الأقراص المحمولة لفترة مؤقتة لحفظ البيانات الشخصية، يجب حفظها في مكان آمن، ويجب تشفير السجل الإلكتروني. وفي حال عدم وجود حاجة للأجهزة المحمولة لحفظ البيانات الشخصية، يجب إلغاء البيانات الشخصية عنها.

14- على مسؤول الاتصالات وتكنولوجيا المعلومات (ICT Officer) التأكد من وضع وتطبيق نظم إستعادة البيانات والنسخ لتشمل كل السجلات الإلكترونية، والتأكد من أن عمليات النسخ (backup) تتم بطريقة دورية ملائمة مع درجة حساسية البيانات الشخصية.

15- على السجلات الإلكترونية أن تكون آلية للسماح بإستعادة البيانات بطريقة سهلة في حال صعوبة عملية النسخ، على سبيل المثال في الظروف مثل انقطاع الكهرباء المتكرر، فشل الأنظمة الإلكترونية، أو الكوارث الطبيعية.

16- في حال عدم وجود حاجة للسجلات الإلكترونية على الهيئة التنسيق مع مسؤول الاتصالات وتكنولوجيا المعلومات (ICT Officer) لإلغاء البيانات.

- عند تقييم مستوى أمان البيانات المنصوص عليه في الفقرة 1/ من هذه المادة، يجب أخذ ما يأتي بالإعتبار:
- 1- المخاطر المصاحبة للمعالجة بما في ذلك تلف البيانات الشخصية أو ضياعها أو التعديل العرضي عليها أو غير القانوني لها أو الإفشاء أو الوصول غير المصرح به لها سواء تم نقلها أو تخزينها أو معالجتها.
 - 2- تكاليف تنفيذ المعالجة وطبيعتها ونطاقها وأعراضها، وكذلك تباين المخاطر المحتملة على خصوصية وسرية البيانات الشخصية لصاحب البيانات.

المادة (16) تقييم أثر حماية البيانات الشخصية:

يجب على الهيئة إجراء تقييم لأثر حماية البيانات (DPIA) عندما يُحتمل أن تشكّل معالجة البيانات الشخصية خطراً على حقوق صاحب البيانات وحرياته. وفي كلّ الأحوال، على الهيئة إجراء تقييم لأثر حماية البيانات قبل نقل أي بيانات إلى طرف ثالث.

من دون الإخلال بطبيعة عملية المعالجة ومداها وأهدافها، يجب على الهيئة، قبل الشروع في المعالجة، إجراء تقييم لأثر المعالجة، وذلك عند استخدام أي من التقنيات الجديدة التي قد تُعرض خصوصية البيانات الشخصية لصاحب البيانات وسريتها للخطر.

ويُعدّ التقييم المنصوص عليه في الفقرة 1/ من هذه المادة ضرورياً في الحالات الآتية:

1. قبل نقل البيانات الشخصية إلى طرف ثالث:
 2. إذا كانت المعالجة تتضمن تقييماً ممنهجاً وشاملاً للجوانب الشخصية لصاحب البيانات التي تعتمد على المعالجة الآلية بما فيها التنبؤ، والتي لها تبعات قانونية أو التي من شأنها أن تؤثر بشكل جسيم على صاحب البيانات.
 3. إذا كانت المعالجة ستتم على كمية كبيرة من البيانات الشخصية الحساسة.
- يجب أن يتضمن التقييم المنصوص عليه في البند الأول من هذه المادة بحدّ أدنى ما يأتي:

- 1- شرح واضح وممنهج لعمليات المعالجة المقترحة على حماية البيانات الشخصية والغرض من معالجتها.
- 2- تقييم مدى ضرورة عمليات المعالجة وتناسبها مع الغرض منها.
- 3- تقييم المخاطر المحتملة على خصوصية وسرية البيانات الشخصية لصاحب البيانات.
- 4- الإجراءات والتدابير المقترحة للحدّ من المخاطر المحتملة على حماية البيانات الشخصية.

يجوز للهيئة إجراء تقييم واحد لمجموعة من عمليات المعالجة التي تتشابه في طبيعتها أو في مستوى المخاطر المرتبطة بها. يجب على الهيئة التأكد من إشراك موظف حماية البيانات (DPO) عند تقييم أثر حماية البيانات الشخصية. كما يجب على الهيئة إعداد قائمة بأنواع عمليات المعالجة التي يُعد إجراء تقييم لأثر حماية البيانات الشخصية فيها إلزامياً، وإتاحة هذه القائمة للجمهور على موقعها الإلكتروني. ويجب على الهيئة مراجعة نتائج التقييم بشكل دوري للتحقق من تنفيذ المعالجة وفقاً لما ورد في التقييم، وذلك في حال تغير مستوى المخاطر المصاحبة لعمليات المعالجة.

المادة (17) تدابير السلامة:

يجب على الهيئة اتخاذ جميع التدابير الفنية والمهنية والتنظيمية، وذلك في ضوء طبيعة البيانات الشخصية والمخاطر الناتجة عن معالجتها، من أجل ضمان سلامة البيانات وحمايتها، ومنع تعرضها للإختراق أو الفساد أو التلف أو الفقدان، أو الوصول إليها من قبل أشخاص غير مخولين، وأي عمليات معالجة غير قانونية أخرى للبيانات.

المادة (18) خرق سلامة البيانات:

يجب على الهيئة معالجة أي خرق لسلامة البيانات من دون تأخير غير مبرر.

يجب على موظف حماية البيانات (DPO) دعم الهيئة من أجل تقديم ما يأتي:

(1) وصف الخرق ونوعه.

(2) وصف النتائج المحتملة للخرق.

(3) وصف الإجراءات التي اتخذها أو ينوي اتخاذها لمعالجة نتائج الخرق وتخفيف آثاره وحماية البيانات ذات الطابع الشخصي.

يجب على موظف حماية البيانات (DPO) الاحتفاظ بسجل لكلّ الخروقات (بما في ذلك، على سبيل المثال لا الحصر، خروقات سلامة البيانات المذكورة في الفقرة (1) أعلاه، وعواقبها، والإجراءات المتخذة لمعالجتها).