



تخاطب هذه الارشادات المتحكم والمعالج للبيانات، ومسؤول حماية البيانات، و مديرو الأشخاص الاعتباريين/القانونيين.



مواد القانون ذات الصلة: 2 و 3 و 4 و 5 و 6 و 37 من قانون حماية البيانات الشخصية، والمواد رقم _____ من اللائحة التنفيذية.

نص القانون على سبعة مبادئ لابد أن يلتزم بها المتحكمين والمعالجين عند القيام بأنشطتهم وهي:

1. المشروعية والشفافية
2. تقييد الغرض
3. تقليص البيانات
4. صحة البيانات
5. مدة التخزين
6. التأمين
7. المساءلة

1. المشروعية والشفافية

1. المشروعية

- 1.1. يجب ألا يخالف جمع البيانات الشخصية ومعالجتها أي من القوانين أو اللوائح.
 - 1.2. يجب أن يكون الأساس القانوني لمعالجة البيانات معينا وموثقا.
- أسس المشروعية تتضمن على سبيل المثال: موافقة الشخص المعني بالبيانات أو التعاقد بين الشخص المعني بالبيانات والمتحكم.

2. الشفافية

- 2.1. يجب على المتحكم تزويد الشخص المعني بالبيانات بجميع المعلومات اللازمة ليتمكن من اتخاذ قرار مستنير بشأن معالجة وجمع بياناته الشخصية.
- 2.2. يجب أن تكون المعلومات المقدمة موجزة ويسهل الوصول إليها وأن تعرض بلغة واضحة وبسيطة الفهم.
- 2.3. يجب التأكد من أن الشخص المعني بالبيانات على دراية بكيفية استخدام بياناته الشخصية من المتحكم أو المعالج.
- 2.4. يجب على المتحكمين إبلاغ الشخص المعني بالبيانات حال تعديل أهداف المعالجة.

2. تقييد الغرض

يجب أن يكون جمع البيانات محدودا أو ملائما للغرض الذي قبل به الشخص المعني بالبيانات. وإذا قرر المتحكم معالجة البيانات لأغراض إضافية، فيلتزم بالحصول على موافقة جديدة من الشخص المعني بالبيانات.

مثال:

إذا حصلت المستشفى على موافقة لجمع بيانات المريض للأغراض الطبية فقط، فلا يمكن للمستشفى استخدام نفس البيانات للتسويق الإلكتروني (مثل الإعلان عن خدمات تجميلية جديدة) دون الحصول على موافقة الشخص المعني بالبيانات.

3. تقليص البيانات

يجب على المتحكمين جمع البيانات اللازمة فقط لإجراء النشاط الذي أعلن به الشخص المعني بالبيانات.

مثال:

لا يحتاج تطبيق اللياقة البدنية الذي يوفر خطط التغذية إلى الحصول على الموقع الجغرافي للمستخدمين لعدم تعلقه بأنشطة التطبيق.

4. صحة البيانات

يجب أن يكون لدى المتحكم سياسة لضمان دقة البيانات، على سبيل المثال: تمكين أصحاب البيانات من تحديث بياناتهم وتصحيحها حسب الضرورة.

مثال:

تحديث موظفي الاستقبال بالعيادات للبيانات الشخصية للمرضى أثناء زيارات المرضى وتحديث السجلات وفقاً لذلك.

5. مدة التخزين

يجب على المتحكمين / المعالجين حذف البيانات فور الانتهاء من الغرض الذي تم جمعها ومعالجتها من أجله، ما لم تستثنى أي قوانين معمول بها أو مصلحة مشروعة لزوم الحذف. في حالة وجود استثناء لشرط الحذف، يجب على المتحكم / المعالج اتخاذ الإجراءات المناسبة للحد من الوصول للبيانات مثل التشفير. كذلك، يجب على المتحكمين الاحتفاظ بسجل لتوثيق أغراض البيانات والمدة التي يهدف إلى استخدام البيانات خلالها.

مثال:

تقوم شركة تجارة إلكترونية بجمع بيانات العملاء لمعالجة الطلبات؛ يجب على الشركة حذف البيانات بمجرد تنفيذ الطلب وانتهاء صلاحية أي فترات إرجاع أو ضمان.

6. التأمين

يجب على المتحكمين / المعالجين استخدام الوسائل التنظيمية والتقنية المناسبة لحماية خصوصية وأمن البيانات الشخصية. ويشمل ذلك وضع سياسة أمنية، وتدريب الموظفين، وضمان التنفيذ الصحيح للتدابير الأمنية، والتحقق الفوري في الحوادث الأمنية.

7. المساءلة

يجب أن يكون المتحكمين / المعالجين قادرين على إثبات الامتثال لجميع مبادئ معالجة البيانات، وذلك بالاحتفاظ بالوثائق المتعلقة بسياسات حماية البيانات والمشروعية؛ والإبقاء على سياسة لحماية البيانات؛ وتسجيل انتهاكات البيانات الشخصية والإبلاغ عنها إلى مركز حماية البيانات الشخصية؛ وتقييم مدى حماية البيانات الشخصية وتحديد الأسباب التي من المحتمل أن تؤدي إلى مخاطر عالية لمصالح الأشخاص المعنيين بالبيانات؛ وتعيين مسؤول حماية البيانات.



عدم الامتثال لهذه المبادئ يعاقب عليه بغرامات تتراوح بين 200,000 جنيه مصري إلى 3,000,000 جنيه مصري.