إتقان
محامون و مستشارون قانونيون

دليل عملي للشركات

# دليل الشركات للامتثال لقانون حماية البيانات الشخصية المصري

قراءة عملية في القانون رقم 151 لسنة 2020 ولائحته التنفيذية رقم 816 لسنة 2025

إصدار 2026

إتقان - محامون ومستشارون قانونيون

إتقان
محامون و مستشارون
قانونيون

# عن هذا الدليل

أعدت إتقان هذا الدليل لمساعدة الشركات على فهم المتطلبات العملية للامتثال لقانون حماية البيانات الشخصية المصري ولائحته التنفيذية، من منظور مؤسسي يجمع بين القانون والحوكمة والتشغيل اليومي.

يقدم الدليل شرحًا مبسطًا ومباشرًا لأهم الالتزامات والمخاطر، مع جداول وقوائم تحقق ونماذج أولية يمكن تطويرها بما يناسب طبيعة كل شركة.

# المحتويات


| | | |
|---|---|---|
| 01 | مقدمة ومنهجية الدليل | 4 |
| 02 | نطاق تطبيق القانون | 5 |
| 03 | المصطلحات الأساسية | 7 |
| 04 | مبادئ وشروط المعالجة | 8 |
| 05 | حقوق أصحاب البيانات | 10 |
| 06 | التزامات المتحكم والمعالج | 12 |
| 07 | مسؤول حماية البيانات | 14 |
| 08 | البيانات الحساسة وبيانات الأطفال | 15 |
| 09 | التسويق الإلكتروني المباشر | 16 |
| 10 | نقل البيانات عبر الحدود | 18 |
| 11 | خرق البيانات الشخصية | 20 |
| 12 | بيانات الموظفين والموارد البشرية | 22 |
| 13 | العقوبات والمخاطر | 23 |
| 14 | خطة امتثال خلال 30 يومًا | 24 |
| 15 | قوائم تحقق للإدارات | 26 |
| 16 | نماذج مختصرة | 28 |
| 17 | المصادر القانونية والمنهجية | 30 |

# لماذا تحتاج الشركات إلى هذا الدليل؟

لم تعد حماية البيانات الشخصية مسألة تقنية تخص قسم تكنولوجيا المعلومات فقط، بل أصبحت التزامًا مؤسسيًا يشترك فيه مجلس الإدارة والإدارة القانونية والموارد البشرية والتسويق والمبيعات وخدمة العملاء.

**المبدأ العملي:**
أي شركة تحتفظ ببيانات عملاء أو موظفين أو موردين أو مستخدمي موقع إلكتروني قد تكون مخاطبة بالتزامات حماية البيانات إذا كانت هذه البيانات تعالج إلكترونيًا كليًا أو جزئيًا.

## الفكرة الأساسية

قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020، ولائحته التنفيذية الصادرة بقرار وزير الاتصالات وتكنولوجيا المعلومات رقم 816 لسنة 2025، يضعان إطارًا لتنظيم جمع البيانات الشخصية ومعالجتها وتخزينها ونقلها وإتاحتها والتسويق الإلكتروني المباشر.

هذا الدليل لا يهدف إلى نقل النصوص القانونية، بل إلى ترجمة الالتزامات إلى خطوات عملية قابلة للتطبيق داخل الشركات.

## ما الذي تغير بعد صدور اللائحة التنفيذية؟

اللائحة التنفيذية حولت كثيرًا من الالتزامات العامة في القانون إلى متطلبات تشغيلية: سجلات إلكترونية مؤمنة، آليات موافقة، تراخيص وتصاريح، متطلبات لمسؤول حماية البيانات، إجراءات للتعامل مع خرق البيانات، وضوابط للتسويق الإلكتروني ونقل البيانات عبر الحدود.

### استجابة
خطة واضحة للطلبات والشكاوى والاختراقات.

### توثيق
سجلات إلكترونية للمعالجة والموافقات والاحتفاظ.

### حوكمة
تحديد الأدوار والمسؤوليات داخليًا.

## لمن هذا الدليل؟

- الإدارة التنفيذية التي تحتاج إلى رؤية واضحة للمخاطر والالتزامات.
- الإدارة القانونية التي تتولى صياغة السياسات والعقود والنماذج.
- إدارة الموارد البشرية التي تتعامل يوميًا مع بيانات الموظفين والمرشحين.
- إدارة التسويق والمبيعات التي تستخدم البريد الإلكتروني وواتساب والرسائل النصية والإعلانات الموجهة.
- إدارة تكنولوجيا المعلومات والأمن السيبراني المسؤولة عن حماية الأنظمة والبيانات.

الفصل 02

# نطاق تطبيق القانون: هل شركتك مخاطبة؟

الخطوة الأولى في أي برنامج امتثال هي تحديد ما إذا كان القانون ينطبق على نشاط الشركة، وما نوع البيانات والعمليات التي تقع داخل نطاقه.

## القاعدة العامة

تسري أحكام القانون على حماية البيانات الشخصية المعالجة إلكترونيًا، جزئيًا أو كليًا، لدى أي حائز أو متحكم أو معالج، وذلك بالنسبة للأشخاص الطبيعيين.

**تطبيق عملي:** إذا كانت الشركة تحتفظ بقاعدة بيانات عملاء على نظام CRM، أو ملفات موظفين على نظام HR، أو طلبات توظيف على بريد إلكتروني أو منصة إلكترونية، فغالبًا نحن أمام معالجة إلكترونية لبيانات شخصية.

## أمثلة على شركات غالبًا تقع داخل النطاق

| نوع الشركة | أمثلة على البيانات | نقطة الخطر |
|---|---|---|
| التجارة الإلكترونية | الأسماء، العناوين، أرقام الهواتف، سجل الطلبات | التسويق وإتاحة البيانات لشركات الشحن والدفع |
| الشركات الخدمية | بيانات العملاء، الشكاوى، العقود، المراسلات | الاحتفاظ غير المحدد أو مشاركة البيانات دون أساس |
| العيادات والمراكز الطبية | بيانات صحية وحجوزات وتقارير | البيانات الصحية تعد من البيانات الحساسة |
| المدارس والمنصات التعليمية | بيانات الطلاب وأولياء الأمور ونتائج الاختبارات | بيانات الأطفال تعامل كبيانات حساسة |
| شركات التسويق | قوائم العملاء المحتملين وسلوك المستخدمين | اشتراطات خاصة للتسويق الإلكتروني المباشر |

## استثناءات مهمة

القانون يستبعد بعض الحالات مثل الاستخدام الشخصي البحت، وبعض المعالجات الإحصائية أو القانونية، والبيانات لدى جهات الأمن القومي، وبعض البيانات لدى البنك المركزي والجهات الخاضعة لرقابته وفق الاستثناءات المحددة قانونًا.

**تنبيه:** الاستثناء لا يطبق بالتوسع. مجرد أن الشركة تعمل في قطاع منظم لا يعني تلقائيًا خروجها من قانون حماية البيانات.

## سؤال تشخيصي سريع

1. هل تجمع الشركة بيانات أشخاص طبيعيين؟
2. هل تحفظ هذه البيانات أو تعالجها إلكترونيًا ولو جزئيًا؟
3. هل تستخدم البيانات لغرض تجاري أو إداري أو تسويقي أو خدمي؟
4. هل يتم الإفصاح عن البيانات لطرف ثالث مثل شركة دفع أو شحن أو مزود سحابي؟

إذا كانت الإجابة بنعم على أي من الأسئلة السابقة، فالخطوة التالية هي إجراء خريطة بيانات داخلية.

الفصل 03

# المصطلحات الأساسية بلغة الشركات

الفهم الصحيح للمصطلحات يحدد المسؤولية القانونية: هل الشركة متحكم؟ معالج؟ حائز؟ أم أكثر من صفة في الوقت ذاته؟

| المصطلح | المعنى العملي | مثال داخل الشركة |
|---|---|---|
| البيانات الشخصية | أي بيانات تخص شخصًا طبيعيًا محددًا أو يمكن تحديده مباشرة أو غير مباشرة. | الاسم، الهاتف، البريد، الصورة، رقم الهوية، عنوان IP، بيانات الوظيفة. |
| البيانات الحساسة | بيانات تحتاج حماية أعلى بسبب طبيعتها أو أثرها على الشخص. | الصحة، القياسات الحيوية، البيانات المالية، المعتقدات، الآراء السياسية، بيانات الأطفال. |
| الشخص المعني بالبيانات | الشخص الذي تخصه البيانات. | عميل، موظف، مرشح لوظيفة، مستخدم موقع، مورد فرد. |
| المتحكم | الجهة التي تحدد الغرض من جمع البيانات وطريقة معالجتها. | شركة تجمع بيانات عملائها لإدارة الخدمة والتسويق. |
| المعالج | جهة تعالج البيانات لصالح المتحكم وبناءً على تعليماته. | شركة استضافة سحابية أو شركة Payroll أو مركز اتصال خارجي. |
| الحائز | من يحوز أو يحتفظ بالبيانات قانونًا أو فعليًا. | أرشيف إلكتروني أو مزود حفظ مستندات. |
| المعالجة | أي عملية إلكترونية على البيانات: جمع، تسجيل، تخزين، تعديل، تحليل، إتاحة، نقل، حذف. | إدخال بيانات العميل على CRM أو إرسال حملة رسائل. |

**ملحوظة عملية:**
الشركة الواحدة قد تكون متحكمًا في بيانات عملائها، ومعالجًا لبيانات شركة أخرى، وحائزًا لبيانات محفوظة لديها. لذلك لا يكفي وضع تصنيف واحد للشركة ككل، بل يجب تقييم كل نشاط معالجة على حدة.

## كيف تحدد صفة شركتك؟

- إذا كنت تحدد لماذا تجمع البيانات وكيف تستخدمها، فأنت غالبًا متحكم.
- إذا كنت تستخدم البيانات فقط لتنفيذ خدمة لصالح طرف آخر ووفق تعليماته، فأنت غالبًا معالج.
- إذا كنت تحتفظ بالبيانات دون تحديد الغرض أو طريقة المعالجة، قد تكون حائزًا.

الفصل 04

# مبادئ وشروط جمع البيانات ومعالجتها

القانون لا يمنع الشركات من استخدام البيانات، لكنه يشترط أن يكون الاستخدام مشروعًا ومحددًا ومعلنًا ومؤمنًا ومتناسبًا مع الغرض.

## الشروط القانونية الأساسية

### الصحة والدقة

يجب أن تكون البيانات صحيحة وسليمة ومحدثة عند اللزوم.

### الغرض المحدد

تجمع البيانات لأغراض مشروعة ومحددة ومعلنة للشخص المعني.

### الأمن والسرية

تتخذ التدابير الفنية والتنظيمية لحماية البيانات.

### التناسب

لا تجمع أكثر مما تحتاجه لتحقيق الغرض المعلن.

### عدم تغيير الغرض

لا تستخدم البيانات لغرض جديد إلا وفق أساس قانوني مناسب.

### الاحتفاظ المحدد

لا تحتفظ بالبيانات لمدة أطول من اللازم.

## الموافقة ليست ورقة شكلية

اللائحة التنفيذية تؤكد أهمية الموافقة، وأن تكون مرتبطة بالغرض، وأن يتم تسجيلها في سجل إلكتروني مؤمن يتضمن تاريخ الموافقة وصورتها والغرض ونطاق الاستخدام.

**خطأ شائع:** استخدام جملة عامة مثل "أوافق على استخدام بياناتي" دون تحديد الغرض، أو استخدام بيانات العميل لاحقًا في التسويق دون موافقة واضحة أو أساس مشروع.

## ما الذي يجب توثيقه؟

| البند | ماذا يوثق؟ |
|---|---|
| الغرض | لماذا تجمع البيانات؟ تقديم خدمة، تنفيذ عقد، توظيف، تسويق، دعم فني. |
| فئات البيانات | بيانات تعريفية، مالية، صحية، بيانات أطفال، بيانات سلوك رقمي. |
| الموافقة | تاريخها، طريقة الحصول عليها، نصها، وسيلة سحبها. |
| مدة الاحتفاظ | المدة أو معيار تحديدها لكل فئة بيانات. |
| الإتاحة للأطراف الثالثة | من يستلم البيانات؟ ولماذا؟ وبأي سند؟ |
| إجراءات الأمن | الصلاحيات، التشفير، النسخ الاحتياطي، مراقبة الدخول، خطة الاستجابة. |

الفصل 05

# حقوق أصحاب البيانات وكيف تتعامل الشركة معها

حقوق الشخص المعني بالبيانات ليست مجرد نصوص نظرية؛ يجب أن يكون لدى الشركة آلية لاستقبال الطلبات والرد عليها وتوثيق ما تم.

## أهم الحقوق

### الوصول

تمكين الشخص من الاطلاع على بياناته بالضوابط القانونية.

### العلم والمعرفة

معرفة البيانات التي تم جمعها والغرض منها.

### المحو

حذف البيانات عند انتهاء الغرض أو سحب الموافقة في الحالات المناسبة.

### التصحيح والتعديل

تصحيح البيانات غير الدقيقة أو استكمال الناقص منها.

### سحب الموافقة

العدول عن موافقة سابقة متى كان ذلك متاحًا قانونًا.

### الاعتراض

الاعتراض على معالجة تمس الحقوق والحريات الأساسية.

## مهلة الرد

يلتزم من يقدم إليه طلب متعلق بممارسة الحقوق بالرد خلال ستة أيام عمل من تاريخ تقديم الطلب، وفقًا للقانون.

**إجراء مقترح:** إنشاء بريد إلكتروني أو نموذج إلكتروني داخلي لطلبات حماية البيانات، مع رقم مرجعي لكل طلب، وسجل يوضح تاريخ الاستلام، نوع الطلب، المسؤول عنه، تاريخ الرد، والنتيجة.

## سير عمل عملي لطلبات أصحاب البيانات

1. **استلام الطلب:** عبر قناة رسمية معلنة.

2. **التحقق من الهوية:** دون طلب بيانات زائدة عن الحاجة.

3. **تصنيف الطلب:** وصول، تصحيح، محو، اعتراض، سحب موافقة.

4. **فحص الأساس القانوني:** هل توجد مدة احتفاظ إلزامية أو التزام قانوني يمنع المحو؟

5. **تنفيذ القرار:** داخل الأنظمة المعنية وإبلاغ الأطراف الثالثة عند اللزوم.

6. **الرد والتوثيق:** خلال المدة القانونية وتسجيل القرار.

الفصل 06

# التزامات المتحكم والمعالج

القانون يميز بين المتحكم والمعالج، لكنه يفرض على كل منهما التزامات مستقلة. لذلك يجب أن تعكس العقود والسياسات الداخلية هذا التمييز.

## التزامات المتحكم

| الالتزام | ترجمته العملية داخل الشركة |
|---|---|
| الحصول على البيانات وفق موافقة أو سند قانوني | نماذج موافقة وسياسات خصوصية واضحة. |
| التأكد من صحة البيانات وكفايتها | مراجعة حقول الإدخال وعدم طلب بيانات غير لازمة. |
| تحديد طريقة ومعايير المعالجة | سياسة داخلية تحدد من يستخدم البيانات ولماذا. |
| اتخاذ تدابير تقنية وتنظيمية للحماية | صلاحيات، تشفير، نسخ احتياطي، تدريب، مراقبة دخول. |
| محو البيانات بعد انتهاء الغرض | جدول احتفاظ وعمليات حذف دورية أو إخفاء هوية. |
| إمساك سجل خاص للبيانات | سجل أنشطة معالجة يتضمن الفئات، الجهات المتلقية، النقل عبر الحدود، الأمن. |
| الحصول على ترخيص أو تصريح من المركز | تقييم ما إذا كان النشاط يتطلب ترخيصًا أو تصريحًا وفق اللائحة. |

## التزامات المعالج

المعالج لا ينبغي أن يتعامل مع البيانات كمالك لها. يجب أن تكون المعالجة وفق عقد مكتوب وتعليمات محددة من المتحكم، مع التزام بالحماية والسرية وعدم تجاوز الغرض.

**عقد معالجة البيانات ضروري**

عند التعامل مع مزود سحابي، شركة تسويق، شركة Payroll، مركز اتصال، شركة استضافة أو دعم فني، يجب تنظيم العلاقة بعقد يتضمن الغرض، المدة، نوع البيانات، إجراءات الأمن، الإخطار بالاختراق، الحذف أو الرد بعد انتهاء الخدمة.

## بنود لا غنى عنها في عقد المعالجة

- وصف البيانات والغرض من المعالجة.
- تعليمات المتحكم ونطاق سلطة المعالج.
- التزامات السرية وتقييد الوصول.
- التدابير الفنية والتنظيمية للحماية.
- الإخطار الفوري بأي خرق أو اشتباه في خرق.
- تنظيم المعالجين الفرعيين Sub-processors.
- إعادة أو حذف البيانات بعد انتهاء العلاقة.
- حق التدقيق والرقابة والتعاون مع المركز.

الفصل 07

# مسؤول حماية البيانات الشخصية

مسؤول حماية البيانات هو نقطة التقاء بين القانون والتشغيل: يراقب الالتزام، يتابع الطلبات والشكاوى، ويتواصل مع المركز عند اللزوم.

## دوره القانوني والعملي

ينص القانون على أن مسؤول حماية البيانات يتولى تنفيذ أحكام القانون ولائحته وقرارات المركز، ومراقبة الإجراءات المعمول بها داخل الكيان، وتلقي الطلبات المتعلقة بالبيانات الشخصية.

### نقطة اتصال

التعامل مع المركز والرد على الطلبات والبلاغات.

### مراقبة الامتثال

تقييم دوري للسياسات والأنظمة والإجراءات.

### التدريب

رفع وعي الموظفين بمتطلبات حماية البيانات.

### إدارة الطلبات

متابعة طلبات الوصول والتصحيح والمحو والاعتراض.

## القيد لدى المركز

اللائحة التنفيذية تنشئ سجلًا إلكترونيًا لمسؤولي حماية البيانات لدى المركز، ويكون لكل مسؤول كود تعريفي، مع متطلبات للقيد مثل المؤهلات أو الشهادات والخبرة واجتياز الاختبارات المعتمدة وعدم الإدانة في الجرائم المخلة بالشرف والأمانة.

## استقلالية مسؤول حماية البيانات

من المهم ألا يكون مسؤول حماية البيانات مجرد اسم شكلي. يجب أن تكون له صلاحيات كافية للوصول إلى المعلومات ومراجعة السياسات وإصدار التوصيات ورفع المخاطر للإدارة.

**خطأ شائع:** تعيين مسؤول IT وحده دون تمكين قانوني أو إداري، أو إسناد المهمة لشخص تتعارض وظيفته مع الرقابة المستقلة على استخدام البيانات.

الفصل 08

# البيانات الحساسة وبيانات الأطفال

البيانات الحساسة تتطلب عناية أعلى، وترخيصًا أو تصريحًا وموافقة واضحة في الحالات التي يحددها القانون، ولا يجوز التعامل معها بنفس منطق البيانات العادية.

## ما هي البيانات الحساسة؟

تشمل البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، والقياسات الحيوية، والبيانات المالية، والمعتقدات الدينية، والآراء السياسية، والحالة الأمنية. وتعد بيانات الأطفال من البيانات الشخصية الحساسة في جميع الأحوال.

## أمثلة عملية

| البيان | لماذا حساس؟ | ماذا تفعل الشركة؟ |
|---|---|---|
| تقارير طبية للموظفين | تتعلق بالصحة | قصر الوصول على HR المخول والاحتفاظ للمدة اللازمة فقط. |
| بصمة حضور وانصراف | بيانات بيومترية | تقييم الضرورة وتطبيق حماية تقنية مشددة. |
| بيانات طلاب أو أطفال | بيانات أطفال | موافقة ولي الأمر وعدم طلب بيانات زائدة عن الحاجة. |
| بيانات مالية تفصيلية | تفصح عن الوضع المالي | تشفير وتقييد الوصول وتحديد الغرض بدقة. |

**قاعدة ذهبية:** قبل جمع أي بيانات حساسة، اسأل: هل هي ضرورية؟ هل يمكن تحقيق الغرض ببيانات أقل؟ هل توجد موافقة واضحة وسند قانوني؟ هل لدينا ترخيص أو تصريح إذا تطلب الأمر؟

## بيانات الأطفال

عند التعامل مع بيانات الأطفال، يلزم موافقة ولي الأمر في الحالات المقررة، كما يجب ألا يكون اشتراك الطفل في لعبة أو مسابقة أو نشاط مشروطًا بتقديم بيانات تزيد على ما هو ضروري للمشاركة.

الفصل 09

# التسويق الإلكتروني المباشر

التسويق أصبح من أكثر مناطق المخاطر في حماية البيانات، خاصة عند استخدام قواعد أرقام أو بريد إلكتروني أو رسائل واتساب دون توثيق مصدر البيانات والموافقة.

## متى نكون أمام تسويق إلكتروني مباشر؟

عندما تستخدم الشركة وسيلة اتصال إلكترونية للترويج لمنتجاتها أو خدماتها أو خدمات الغير، مثل البريد الإلكتروني أو الرسائل النصية أو واتساب أو الإشعارات أو أي وسيلة رقمية مشابهة.

## التزامات أساسية

- الحصول على ترخيص من المركز لمباشرة نشاط التسويق الإلكتروني المباشر وفق الفئات المحددة في اللائحة.
- الحصول على موافقة صريحة من الشخص المعني بالبيانات على تلقي الاتصال التسويقي.
- عدم استخدام البيانات لغرض آخر أو مشاركتها لأغراض أخرى إلا بموافقة صريحة.
- الاحتفاظ بسجلات إلكترونية تتضمن كيفية وتاريخ الحصول على الموافقة والغرض منها.
- توفير آلية واضحة وسهلة للرفض أو العدول عن الموافقة.
- محو البيانات عند العدول عن الموافقة أو انتهاء مدة الاحتفاظ أو انتفاء الغرض التسويقي.

**مخاطر شائعة:** شراء قواعد بيانات أرقام، إرسال رسائل دعائية لعملاء سابقين دون موافقة تسويقية منفصلة، أو عدم توفير رابط/طريقة واضحة لإلغاء الاشتراك.

## Checklist قبل أي حملة تسويقية

| | |
|---|---|
| ☐ | هل نعرف مصدر بيانات الاتصال؟ |
| ☐ | هل توجد موافقة صريحة موثقة على التسويق؟ |
| ☐ | هل الرسالة توضح أنها لأغراض تسويقية؟ |
| ☐ | هل توجد طريقة سهلة للرفض أو إلغاء الاشتراك؟ |
| ☐ | هل لدينا سجل بالموافقة وطلبات العدول عنها؟ |
| ☐ | هل الحملة متوافقة مع نطاق الترخيص أو التصريح؟ |

الفصل 10

# نقل البيانات الشخصية عبر الحدود

كثير من الشركات تنقل البيانات خارج مصر دون أن تنتبه: استخدام خدمات Cloud، أدوات CRM، بريد إلكتروني مستضاف خارجيًا، أدوات تحليل المواقع، أو شركات دعم فني خارجية.

## ما المقصود بالنقل عبر الحدود؟

هو نقل أو مشاركة أو تخزين أو معالجة أو إتاحة بيانات شخصية تم جمعها أو تجهيزها للمعالجة داخل مصر إلى خارج النطاق الجغرافي لجمهورية مصر العربية.

## أمثلة عملية

- استضافة قاعدة العملاء على خوادم خارج مصر.
- استخدام مزود CRM أو Email Marketing عالمي.
- إرسال بيانات موظفين إلى شركة أم خارج مصر.
- منح فريق دعم فني خارج مصر حق الدخول إلى نظام يحتوي على بيانات شخصية.
- استخدام أدوات تحليلات تجمع معرفات مستخدمين أو بيانات سلوك رقمي.

## متطلبات عملية وفق اللائحة

تتطلب اللائحة عند طلب ترخيص أو تصريح النقل عبر الحدود تحديد الوجهة، طبيعة نشاط الطرف المستقبل، طبيعة البيانات، نظم التأمين وأماكن التخزين المؤقتة والنهائية، الغرض من النقل، وصف فئات البيانات وحجمها ومدة الاحتفاظ بها.

**قبل التعاقد مع مزود خارجي:** اطلب منه مستندات الأمن والامتثال، أماكن التخزين، آليات الحذف، قائمة المعالجين الفرعيين، إجراءات الإخطار بالاختراق، وشروط نقل البيانات لدول أخرى.

# خريطة بيانات النقل الخارجي

| النظام/المورد | الدولة | نوع البيانات | الغرض | مدة الاحتفاظ | إجراءات الأمن |
|---|---|---|---|---|---|
| CRM | يحدد | عملاء ومراسلات | إدارة علاقات العملاء | حسب السياسة | تشفير وصلاحيات |
| Email Marketing | يحدد | بريد وأسماء | حملات تسويقية | حتى سحب الموافقة | سجلات موافقة وحذف |
| Cloud Storage | يحدد | مستندات تشغيلية | تخزين ومشاركة داخلية | حسب الفئة | MFA ومراقبة دخول |

الفصل 11

# خرق أو انتهاك البيانات الشخصية

التعامل مع خرق البيانات يحتاج خطة مسبقة. أسوأ لحظة لوضع خطة هي بعد وقوع الاختراق.

## متى يحدث الخرق؟

قد يحدث الخرق عند فقدان أو إتاحة أو إفشاء أو تعديل أو إتلاف غير مشروع للبيانات، أو عند الدخول غير المصرح به إلى أنظمة تحتوي على بيانات شخصية.

## أمثلة

- إرسال ملف عملاء بالخطأ إلى مستلم غير مصرح له.
- اختراق حساب بريد إلكتروني يحتوي على بيانات عملاء أو موظفين.
- فقدان جهاز أو وسيط تخزين غير مشفر.
- إتاحة رابط تحميل يحتوي على بيانات دون صلاحيات.
- هجوم Ransomware على قاعدة بيانات الشركة.

## المهلة القانونية

تلتزم الشركة، بحسب صفتها كمتحكم أو معالج، بإبلاغ المركز خلال اثنتين وسبعين ساعة من تاريخ العلم بالخرق أو الانتهاك. كما تلتزم بإخطار الشخص المعني بالبيانات خلال ثلاثة أيام عمل من تاريخ إبلاغ المركز، مع بيان إجراءات التأمين المتخذة وبالوسيلة المتفق عليها.

**0-24 ساعة**

عزل الحادث، حفظ الأدلة، تكوين فريق الاستجابة.

**24-48 ساعة**

تحديد نوع البيانات وعدد المتأثرين وتقييم الضرر.

**حتى 72 ساعة**

إبلاغ المركز عبر الوسائل التي يحددها.

**3 أيام عمل**

إخطار أصحاب البيانات بعد إبلاغ المركز.

## سجل الخرق

| ما يجب تسجيله | لماذا؟ |
|---|---|
| تاريخ وساعة العلم بالخرق | لحساب مهلة 72 ساعة. |
| وصف طبيعة الخرق وتوقيته | لفهم نطاق الحادث ومسؤوليته. |
| عدد تقريبي للبيانات المتأثرة | لتقدير المخاطر والضرر. |
| الإجراءات المتخذة | لإثبات السيطرة وتقليل الضرر. |
| إخطارات المركز والأشخاص | لتوثيق الالتزام بالمواعيد. |

**مهم:** عدم الإخطار لا يخفي الخرق؛ غالبًا يزيد المخاطر القانونية والتنظيمية والتجارية.

الفصل 12

# بيانات الموظفين والموارد البشرية

ملفات الموظفين من أكثر مصادر البيانات الشخصية داخل الشركات، وغالبًا تحتوي على بيانات حساسة دون ضوابط كافية.

## ما الذي تتعامل معه HR يوميًا؟

- صور بطاقات وجوازات وشهادات ومؤهلات.
- عقود عمل وبيانات رواتب وحسابات بنكية.
- تقارير طبية أو إجازات مرضية.
- بيانات حضور وانصراف وربما بيانات بيومترية.
- تقييمات أداء وتحقيقات داخلية وجزاءات.
- بيانات مرشحين لم يتم تعيينهم.

## مبادئ عملية للـ HR

| الممارسة | المطلوب |
|---|---|
| التوظيف | إخطار المرشح بالغرض من جمع بياناته ومدة الاحتفاظ بالسيرة الذاتية. |
| ملفات الموظفين | قصر الوصول على المختصين وتحديد مدة الاحتفاظ بعد انتهاء الخدمة. |
| البيانات الصحية | تصنيفها كحساسة وتقليل تداولها داخليًا. |
| كاميرات المراقبة | وضع إشعارات واضحة وتحديد غرض أمني مشروع وعدم استخدامها خارج الغرض. |
| التحقيقات الداخلية | تحديد صلاحيات الوصول وحفظ السجلات وفق الحاجة القانونية. |

**نقطة عملية:**
لا ينبغي الاحتفاظ ببيانات المرشحين إلى أجل غير مسمى. الأفضل وجود سياسة مدة احتفاظ للسير الذاتية وطلبات التوظيف، مع خيار موافقة المرشح على الاحتفاظ ببياناته لفرص مستقبلية.

الفصل 13

# العقوبات والمخاطر

عدم الامتثال لا ينتج عنه غرامات فقط، بل قد يسبب شكاوى، تفتيشًا، تعطيل نشاط تسويقي، وفقدان ثقة العملاء والشركاء.

## نظرة عامة على بعض العقوبات

| المخالفة | المخاطر العقابية وفق القانون |
|---|---|
| جمع أو معالجة أو إفشاء بيانات شخصية في غير الأحوال المصرح بها أو دون موافقة | غرامة لا تقل عن 100 ألف جنيه ولا تجاوز مليون جنيه، وقد تشدد إذا ارتكبت لمنفعة أو بقصد الضرر. |
| الامتناع دون مقتض عن تمكين الشخص من ممارسة حقوقه | غرامة لا تقل عن 100 ألف جنيه ولا تجاوز مليون جنيه. |
| الإخلال بواجبات المتحكم أو المعالج | غرامة لا تقل عن 300 ألف جنيه ولا تجاوز 3 ملايين جنيه. |
| إخلال الممثل القانوني للشخص الاعتباري بواجباته | غرامة لا تقل عن 200 ألف جنيه ولا تجاوز مليوني جنيه. |
| إخلال مسؤول حماية البيانات بمهامه | غرامة لا تقل عن 200 ألف جنيه ولا تجاوز مليوني جنيه، وتقل في حالة الإهمال وفق النص. |
| التعامل غير المشروع مع بيانات شخصية حساسة | الحبس مدة لا تقل عن ثلاثة أشهر وغرامة لا تقل عن 500 ألف جنيه ولا تجاوز 5 ملايين جنيه أو إحدى العقوبتين. |

## المخاطر غير المباشرة

- تعطيل الحملات التسويقية بسبب عدم وجود موافقات موثقة.
- رفض موردين أو شركات أجنبية التعامل بسبب ضعف الامتثال.
- نزاعات مع موظفين أو عملاء بسبب الاحتفاظ أو الإفصاح غير المبرر.
- تكلفة احتواء الاختراقات والتحقيقات الفنية والقانونية.
- ضرر السمعة وفقدان الثقة.

**تذكير:** جدول العقوبات في هذا الدليل إرشادي ومختصر، ويجب الرجوع إلى النص القانوني الكامل عند تقييم أي حالة محددة.

# خطة امتثال عملية خلال 30 يومًا

ليس مطلوبًا أن تبدأ الشركة بمشروع ضخم ومعقد. يمكن بناء خط أساس للامتثال خلال 30 يومًا ثم تطويره تدريجيًا.

### الأسبوع الأول

#### خريطة البيانات

حصر الأنظمة، فئات البيانات، مصادرها، أغراض استخدامها، الأطراف التي تصل إليها، ومواقع التخزين.

### الأسبوع الثاني

#### الفجوات القانونية

تحديد أساس كل معالجة، مراجعة الموافقات وسياسة الخصوصية والعقود مع الموردين، وتصنيف البيانات الحساسة.

### الأسبوع الثالث

#### السياسات والسجلات

إعداد سجل أنشطة المعالجة، سياسة الاحتفاظ، آلية طلبات أصحاب البيانات، وإجراءات التسويق الإلكتروني.

### الأسبوع الرابع

#### الأمن والاستجابة

مراجعة الصلاحيات، اعتماد خطة الاستجابة للخرق، تدريب الإدارات، وتحديد مسؤول حماية البيانات أو فريق الخصوصية.

## مخرجات الشهر الأول

| | |
|---|---|
| ☐ | خريطة بيانات مبدئية للشركة. |
| ☐ | سجل أنشطة معالجة مبدئي. |
| ☐ | سياسة خصوصية محدثة للعملاء/الموقع. |
| ☐ | نموذج موافقة أو آلية موافقة موثقة. |
| ☐ | آلية طلبات أصحاب البيانات. |
| ☐ | قائمة موردي البيانات وعقود المعالجة. |
| ☐ | خطة أولية للتعامل مع خرق البيانات. |
| ☐ | توصية بشأن الترخيص/التصريح ومسؤول حماية البيانات. |

الفصل 15

# قوائم تحقق مختصرة للإدارات

> الامتثال الحقيقي لا يحدث داخل الإدارة القانونية وحدها. كل إدارة تمسك جزءًا من سلسلة البيانات.

## Checklist للإدارة القانونية

| | |
|---|---|
| ☐ | مراجعة سياسة الخصوصية وشروط الاستخدام. |
| ☐ | إضافة بنود حماية بيانات في عقود العملاء والموردين. |
| ☐ | إعداد نموذج عقد معالجة بيانات. |
| ☐ | تقييم متطلبات الترخيص والتصريح. |
| ☐ | إعداد سجل لطلبات أصحاب البيانات والشكاوى. |

## Checklist للموارد البشرية

| | |
|---|---|
| ☐ | تحديث نماذج التوظيف وإخطار المرشحين بالغرض ومدة الاحتفاظ. |
| ☐ | تقييد الوصول إلى ملفات الموظفين. |
| ☐ | تحديد مدة الاحتفاظ ببيانات الموظفين السابقين. |
| ☐ | التعامل الحذر مع التقارير الطبية والبيانات الحساسة. |

## Checklist للتسويق

| | |
|---|---|
| ☐ | عدم استخدام أي قائمة بيانات إلا بعد التحقق من مصدرها والموافقة. |
| ☐ | إتاحة آلية واضحة لإلغاء الاشتراك. |
| ☐ | حفظ سجل بالموافقات وطلبات العدول. |
| ☐ | تقييم الحاجة إلى ترخيص التسويق الإلكتروني المباشر. |

## Checklist لتكنولوجيا المعلومات

| | |
|---|---|
| ☐ | تفعيل MFA للأنظمة التي تحتوي على بيانات شخصية. |
| ☐ | مراجعة صلاحيات الوصول دوريًا. |
| ☐ | تشفير الأجهزة والنسخ الاحتياطية المناسبة. |
| ☐ | تسجيل ومراقبة الدخول إلى الأنظمة الحساسة. |
| ☐ | اختبار خطة الاستجابة للحوادث. |

# نماذج مختصرة قابلة للتطوير

هذه النماذج ليست بديلًا عن الصياغة القانونية التفصيلية، لكنها تساعد الشركة على بناء مستنداتها الأساسية.

## نموذج بند خصوصية مختصر في نموذج جمع البيانات

نحيطكم علمًا بأن البيانات الشخصية المقدمة من جانبكم ستُجمع وتُعالج لغرض [تحديد الغرض]، ولن تستخدم في غير هذا الغرض إلا وفقًا للقانون أو بعد الحصول على موافقتكم عند اللزوم. ويحق لكم ممارسة الحقوق المقررة قانونًا بشأن بياناتكم الشخصية من خلال التواصل عبر [قناة التواصل المخصصة].

## نموذج سجل موافقة

| البيان | الوصف |
|---|---|
| اسم الشخص/المعرف | رقم عميل أو بريد إلكتروني أو معرف داخلي. |
| نص الموافقة | النص المعروض وقت الحصول على الموافقة. |
| الغرض | الخدمة، التسويق، التوظيف، الدعم. |
| التاريخ والوقت | تاريخ وساعة الموافقة. |
| الوسيلة | نموذج إلكتروني، عقد، رسالة، تسجيل. |
| سحب الموافقة | تاريخ السحب والإجراء المتخذ. |

## نموذج إخطار داخلي بواقعة خرق

**تاريخ وساعة اكتشاف الواقعة: [●]**

**النظام أو المصدر المتأثر: [●]**

**نوع البيانات المحتمل تأثرها: [●]**

**عدد تقريبي للأشخاص المتأثرين: [●]**

**الإجراءات العاجلة المتخذة: [●]**

**هل تم تصعيد الواقعة لمسؤول حماية البيانات/الإدارة القانونية؟** [نعم/لا]

## نموذج طلب صاحب بيانات

| | |
|---|---|
| ☐ | طلب اطلاع/وصول إلى البيانات. |
| ☐ | طلب تصحيح أو تعديل. |
| ☐ | طلب محو. |
| ☐ | اعتراض على المعالجة. |
| ☐ | سحب موافقة سابقة. |

ملحق

# المصادر القانونية والمنهجية

تم إعداد هذا الدليل كأداة توعوية عملية للشركات، بالاستناد إلى الإطار القانوني المصري المنظم لحماية البيانات الشخصية.

## المصادر القانونية الأساسية

- القانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية.
- قرار وزير الاتصالات وتكنولوجيا المعلومات رقم 816 لسنة 2025 بإصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية.
- النصوص ذات الصلة بالتزامات المتحكم والمعالج ومسؤول حماية البيانات وحقوق الشخص المعني والتسويق الإلكتروني ونقل البيانات عبر الحدود والإخطار عن الخروقات والعقوبات.

## تنبيه قانوني

هذا الدليل مخصص لأغراض التوعية العامة ولا يعد رأيًا قانونيًا أو بديلًا عن استشارة قانونية متخصصة بشأن حالة محددة. تختلف متطلبات الامتثال بحسب طبيعة النشاط، نوع البيانات، أطراف المعالجة، حجم البيانات، الأنظمة المستخدمة، والقرارات أو النماذج أو التعليمات التي قد تصدر عن مركز حماية البيانات الشخصية.

إتقان

محامون و مستشارون
قانونيون

# تواصل معنا

للاطلاع على المزيد من الأدلة القانونية والتحديثات المهنية

www.itqanlaw.com

لينكدإن
Itqan Law Firm

فيسبوك
صفحة إتقان الرسمية

واتساب
+20 105 050 3390

إكس
@itqanlawfirm

تم إعداد هذا الدليل لأغراض التوعية العامة،
ولا يغني عن استشارة قانونية متخصصة بحسب كل حالة.