



# حماية البيانات

لمحة موجزة



+C  
IFRC

## تعريف حماية البيانات

مجموعة من المبادئ والممارسات لضمان جمع البيانات الشخصية واستخدامها وحمايتها بطريقة تراعي خصوصية الأفراد وأي مخاطر قد تهددهم نتيجة عدم حماية بياناتهم بشكل كافٍ.

## مفاهيم حماية البيانات



**المعالجة:** عملية تناول البيانات الشخصية بالجمع والتخزين والاستخدام والتحليل والحذف،... الخ.



**البيانات الشخصية:** البيانات الشخصية: المعلومات التي تتعلق بمعيشة محددة أو قابلة للتحديد ، أو بشخص معين: الاسم ، والعنوان ، والجنس ، والعمر ، ورقم التعريف ، والصورة ، وبصمة الإصبع ، وما إلى ذلك أيضًا معلومات أكثر حساسية: الحالة الصحية ، والانتماءات الدينية أو السياسية أو التوجه الجنسي. ومن المهم أن نعرف أن هذه القائمة ليست حصرية، فكل ما هو شخصي أو حتى حساس يمكن أن يتغير اعتمادًا على الظروف السياسية أو الاجتماعية أو الاقتصادية.



**المشاركة:** السماح بالحصول على المعلومات عن طريق إرسالها عبر البريد الإلكتروني أو تزويد رابط إليها، أو إعطاء نسخة منها إلى شخص ما، أو السماح بالنفذ إلى قاعدة بيانات بشكل مباشر أو غير مباشر.

### لا تفعل

- لا تستخدم منصات ملفات Dropbox عامة أو منصات Google Drive/Docs متاحة للوصول العام، أو غير ذلك من المنصات الإلكترونية، لمشاركة وثائق تتضمن بيانات شخصية (أو أي بيانات حساسة أخرى)، أو استخدامها بشكل متزامن من قبل عدة أطراف، لا سيما إذا كانت هذه الوثائق غير محمية بكلمة مرور.
- لا تقم بمشاركة ملفات تتضمن بيانات شخصية مع جهات حكومية أو أي شريك آخر، أو تسمح لهم بالوصول إليها، دون النظر أولاً في عواقب ذلك، أو دون إضفاء طابع رسمي على شروط القيام بذلك.
- لا تنشر تفاصيل شخصية (بما في ذلك الصور الفوتوغرافية) للأشخاص المتضررين على حسابات وسائل التواصل الاجتماعي، سواء بشكل شخصي أو مهني، دون سابق اتفاق مع فريق الإعلام والاتصالات والفريق القانوني في منطقتك.
- لا تترك ملفات تتضمن بيانات شخصية (أو أي بيانات حساسة أخرى) في أماكن مفتوحة. احتفظ بها، عند عدم استخدامها، داخل خزانات أو أدراج أو مكاتب مغلقة.
- لا تستخدم وحدات التخزين (USB) لحفظ البيانات الشخصية (أو أي بيانات حساسة أخرى) ما لم يكن المحتوى محمياً بكلمة مرور و/أو مُشفراً.
- لا تفترض أن مجرد طلب الموافقة من فرد، أو ما إذا كان يوافق على شيء ينطوي على استخدام بياناته الشخصية، يُعد كافياً لك من الناحية القانونية أو الأخلاقية لتبدأ عملك. فالموافقة لا تُعطى بسهولة عندما يكون توفير المعونة الضرورية مشروطاً بها.

### افعل

- حدد البيانات الشخصية التي لا بد من جمعها قبل تنفيذ أي مشروع.
- خذ في الاعتبار العادات المحلية والسياق السياسي عند تحديد البيانات الشخصية التي يتعين جمعها، وكيفية شرح الغرض (الأغراض) من جمعها.
- خذ في الاعتبار أن بيانات الموقع والبيانات الديموغرافية، يمكن أن تكون بالغة الحساسية وأن تعرض الأفراد والمجموعات إلى الأذى، حتى وإن لم تكن شخصية بالضرورة.
- حدد المعلومات التي سيُزوّد بها الأشخاص المتضررون. على سبيل المثال: الغرض من المشروع، وسبب جمع البيانات، وكيفية استخدامها، ومن سيطلع عليها، والجهة التي يمكن الاتصال بها للاستفسار عن البيانات الشخصية.
- عند تقديم معلومات أو الحصول على موافقة، احتفظ بسجل بالتفاعلات ذات الصلة، بما في ذلك: وصف المعلومات التي جرى تقديمها، ومن الذي قدّمها، وتاريخ ومكان تقديمها، ومن الذين جرت مقابلتهم، والاعتراضات التي تكون قد أُثيرت.
- حدد الشخص الذي سيكون مسؤولاً عن الإجابة عن الأسئلة حول استخدام البيانات الشخصية وتخزينها وتصحيحها ... الخ.
- قم بتشفير، و/أو وضع كلمة مرور لحماية الأجهزة والملفات الرقمية التي تتضمن بيانات شخصية أو أي بيانات حساسة أخرى (على سبيل المثال، الملفات بصيغة وورد وإكسل وما إلى ذلك).
- خطط لمصير البيانات الشخصية بمجرد أن تنتفي الحاجة إليها. على سبيل المثال، هل سيجري حفظها في ملفات المحفوظات، أو حذفها/محوها بطريقة آمنة؟
- قم بتوفير الوصول إلى الملفات الرقمية أو الورقية التي تحتوي على بيانات شخصية فقط للموظفين (أو المتطوعين أو المستشارين أو غيرهم من الوكلاء المعتمدين) الذين يحتاجون إلى الوصول من أجل القيام بعملهم.
- احتفظ بكلمات المرور والأقفال المادية وجدوان الحماية وبرامج الحماية من الفيروسات الإلكترونية والبرمجيات الضارة، وأي شكل آخر من أشكال الأمان لأجهزة الكمبيوتر أو الهواتف المحمولة أو خزانات الملفات أو الأماكن الأخرى التي سيتم فيها تخزين البيانات الشخصية.
- قم بإعداد اتفاق مكتوب قبل مشاركة أي بيانات شخصية (أو أي بيانات حساسة أخرى) مع طرف آخر خارج منطقتك.



يرجى ملاحظة أنه لا يُقصد بهذه المعلومات أن تكون شاملة. فهناك العديد من مجالات حماية البيانات التي لا يغطيها هذا المنشور. اطلب دائماً المشورة القانونية إذا كانت لديك أسئلة حول تفسير و/أو تنفيذ ممارسات تتعلق بحماية البيانات.