

كيف تؤثر اللائحة العامة لحماية البيانات في مجتمعات المصدر المفتوح؟

روبن مويلفيك



المخلص:

يناقش المقال أثر اللائحة العامة لحماية البيانات في مشروعات المصدر المفتوح ومجتمعاتها، عند معالجة معلومات المشاركين عبر المواقع والمنتديات والنماذج. ويعرض جوانب تتعلق بنطاق التطبيق والموافقة وحقوق الوصول والمحو والإخطار بالخرق وتوثيق أنشطة المعالجة، وما تحتاجه المنصات من وظائف مساندة. ويبين أن إدارة المجتمع العالمي تستدعي النظر في الخصوصية والبيانات، وليس في الشيفرة وحدها. وتوضح الملاحظات المصاحبة الفرق بين الأسس القانونية للمعالجة، وشروط التطبيق خارج الاتحاد، وإبلاغ السلطة الرقابية وإبلاغ الأفراد. ويقدم المقال توعية تاريخية ببعض المتطلبات، مع إبقاء التبسيطات منسوبة إلى المصدر وعدم اعتبار العرض دليلًا شاملًا للامتثال. وتبرز أهميته في ربط الحوكمة التقنية بالإجراءات والقدرة على الاستجابة لحقوق المشاركين.

الكلمات المفتاحية: حماية البيانات، (GDPR)، مجتمعات المصدر المفتوح، الخصوصية، حوكمة البيانات

تدخل اللائحة العامة لحماية البيانات حيز التطبيق في 25 مايو 2018. وسيؤثر هذا التنظيم الجديد للاتحاد الأوروبي في كيفية حماية المؤسسات للبيانات الشخصية عالميًا، وقد يشمل ذلك مشروعات المصدر المفتوح ومجتمعاتها.

تفاصيل اللائحة:

أقر البرلمان الأوروبي اللائحة العامة لحماية البيانات (GDPR) في 14 أبريل 2016، وبدأ إنفاذها في 25 مايو 2018. وهي تحل محل توجيه حماية البيانات (95/46/EC)، الذي صُمم لتوحيد قوانين خصوصية البيانات في أوروبا، وحماية خصوصية بيانات مواطني الاتحاد وتعزيز قدرتهم على التحكم فيها، وإعادة تشكيل طريقة تعامل المؤسسات في المنطقة مع هذه الخصوصية.

وتهدف اللائحة إلى حماية البيانات الشخصية للأفراد داخل الاتحاد في عالم يزداد اعتمادًا على البيانات.

على من تنطبق:

من أكبر التغييرات توسيع النطاق الإقليمي. ويقول المؤلف إن اللائحة تنطبق على جميع المؤسسات التي تعالج البيانات الشخصية لأشخاص يقيمون في الاتحاد، بصرف النظر عن موقع المؤسسة.

تركز غالبية المقالات على شركات تبيع سلعًا أو خدمات، لكن يمكن النظر إلى النطاق الإقليمي من زاوية مشروعات المصدر المفتوح. وهناك صور مختلفة، كشركة برمجيات ربحية تدير مجتمعًا، أو مؤسسة غير ربحية تتمثل في مشروع مفتوح المصدر ومجموعه. وعندما يعمل المجتمع عالميًا، فمن المرجح أن يشارك فيه أشخاص موجودون في الاتحاد.

وإذا كان له حضور على الإنترنت، بموقع أو منتدى أو نظام لتتبع المسائل ونحوها، فغالبًا ما يعالج بيانات شخصية لهؤلاء الأشخاص، مثل الأسماء وعناوين البريد، وربما أكثر. ومن هنا تبرز ضرورة النظر في الامتثال لللائحة.

التغييرات وأثرها:

تعزز (GDPR) حماية بيانات الأشخاص في الاتحاد وخصوصيتهم مقارنة بالتوجيه السابق. ولبعض التغييرات أثر مباشر في المجتمع الذي وصفناه. لننظر إلى بعضها.

الموافقة:

لنفترض أن المجتمع يستخدم منتدى لأعضائه، ونموذج تسجيل واحدًا أو أكثر في موقعه. لن يكفي بعد اللائحة الاعتماد على سياسة خصوصية وشروط طويلة عسيرة القراءة. ينبغي، بحسب المؤلف، الحصول على موافقة صريحة لكل غرض محدد، سواء التسجيل في المنتدى أو في أحد النماذج. ويجب أن تكون الموافقة حرة ومحددة ومستتيرة ولا لبس فيها.

قد يتضمن النموذج مربع اختيار غير محدد مسبقًا، مع نص واضح يبين أغراض استخدام البيانات، ويفضل ربطه بملحق لسياسة الخصوصية وشروط الاستخدام القائمتين.

حق الوصول:

توسع اللائحة حقوق الأشخاص في الاتحاد، ومنها سؤال المؤسسة عما إذا كانت تعالج بياناتهم، وأين، وما البيانات المعالجة. وينبغي تقديم نسخة مجانية عند الطلب، على أن تكون بصيغة إلكترونية إذا طلب صاحب البيانات ذلك.

الحق في النسيان:

يُعرف أيضًا بحق محو البيانات. ويعني أن على المؤسسة، ضمن قيود معينة، حذف بيانات الشخص، وربما وقف أي معالجة إضافية لها، بما فيها معالجة الأطراف الثالثة المرتبطة بالمؤسسة.

وتعني هذه التغييرات الثلاثة أن برمجيات منصتك أو منصاتك تحتاج إلى وظائف تساعد على الامتثال: الحصول على الموافقة وحفظها، واستخراج البيانات وتقديم نسخة إلكترونية لصاحبها، ومحو بيانات شخص محدد.

الإخطار بخرق البيانات:

يصف الأصل الخرق بأنه أخذ البيانات الشخصية أو سرقتها من دون إذن صاحبها، ويذكر إخطار أفراد المجتمع المتأثرين خلال 72 ساعة من اكتشافه، إلا إذا كان من غير المرجح أن يهدد حقوق الأفراد وحرابتهم، ويعد الإخطار إلزامياً.

سجل المعالجة:

تصبح المؤسسة مسؤولة، في عرض المؤلف، عن الاحتفاظ بسجل يتضمن أوصافاً تفصيلية للإجراءات والأغراض وغيرها من وجوه معالجة البيانات الشخصية. ويستخدم السجل لإثبات الامتثال لمتطلب توثيق أنشطة المعالجة ولأغراض التدقيق.

الغرامات:

قد تواجه المؤسسات غير الممتثلة غرامة تصل إلى 4% من رقم أعمالها السنوي العالمي أو عشرين مليون يورو، أيهما أكبر. وهذا الحد الأقصى لأشد المخالفات، مثل عدم توافر موافقة كافية لمعالجة بيانات العملاء أو انتهاك جوهر مبادئ الخصوصية بحكم التصميم، وفق العرض المنقول في الأصل.

كلمات أخيرة:

لا ينبغي استخدام مقالي بوصفه استشارة قانونية أو دليلاً نهائياً للامتثال. تناولت بعض الجوانب التي قد تؤثر في مجتمع مفتوح المصدر، بهدف رفع الوعي باللائحة وأثرها. وبالطبع، تتضمن اللائحة الكثير مما تحتاج إلى معرفته وربما الامتثال له.

ويمكنك استنتاج ضرورة اتخاذ خطوات إذا كنت تدير مجتمعاً عالمياً. وإذا كنت تطبق بالفعل معايير أمن قوية، مثل (ISO 27001) أو (NIST) أو (PCI DSS)، فستكون لديك نقطة انطلاق أفضل.

ولمزيد من المعلومات أحال الأصل إلى: بوابة (GDPR)؛ والنص الرسمي لللائحة الاتحاد الأوروبي 2016/679 بما فيه الترجمات؛ ومقال «ما (GDPR)؟ ثمانية أمور ينبغي للقادة معرفتها»؛ ومقال «كيف تتجنب تدقيق امتثال (GDPR): أفضل الممارسات»، وكلاهما في (The Enterprisers Project). وترد هذه المصادر في المراجع أدناه.

المراجع:

- <https://www.eugdpr.org/eugdpr.org.html>
- <https://www.eugdpr.org/key-changes.html>
- <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1520531479111&uri=CELEX:32016R0679>
- <https://enterpriseproject.com/article/2018/4/what-gdpr-8-things-leaders-should-know>
- <https://enterpriseproject.com/article/2017/9/avoiding-gdpr-compliance-audit-best-practices>