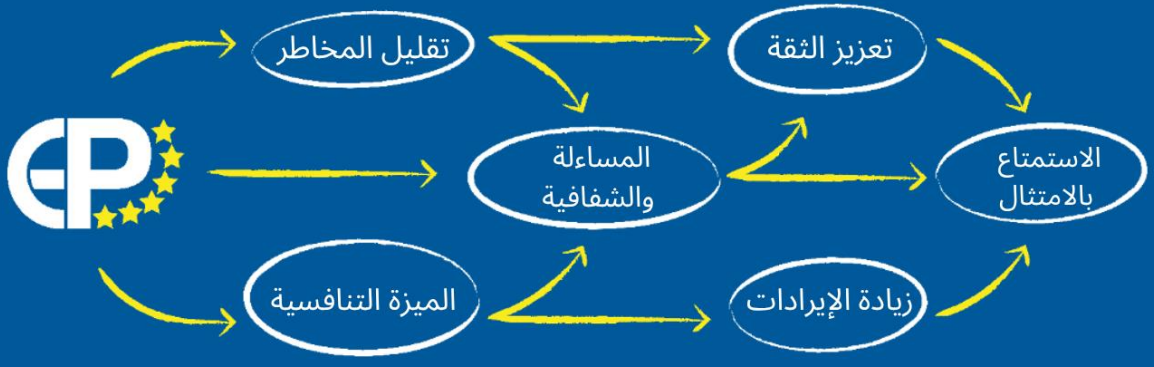
Europrivacy™®

ورقة بيضاء حول شهادة الامتثال للائحة العامة لحماية البيانات (GDPR)

لبناء الثقة وتقليل المخاطر وتعزيز قيمة الامتثال!



المعرف: EP-WP.GC
الإصدار: 1.0
التاريخ: 30 أبريل 2025
المواقع الإلكترونية: www.eccpcenter.org
www.europrivacy.com

معلومات الاتصال: contact@europrivacy.com

الفهرس

مقدمة

تقدم هذه الورقة البيضاء نظرة عامة على شهادة الامتثال للائحة العامة لحماية البيانات (GDPR) مع التركيز على الختم الأوروبي لحماية البيانات.

الاختصارات

الاختصارات	الاسم الكامل
EA	المنظمة الأوروبية للاعتماد
ECCP	المركز الأوروبي للشهادات والخصوصية
EDPB	المجلس الأوروبي لحماية البيانات
EEA	المنطقة الاقتصادية الأوروبية
EU	الاتحاد الأوروبي
GDPR	اللائحة العامة لحماية البيانات
IAF	المنتدى الدولي للاعتماد
ISO	المنظمة الدولية للتوحيد القياسي

تأثير اللائحة العامة لحماية البيانات (GDPR)

أدى بدء سريان اللائحة العامة لحماية البيانات (GDPR) وغراماتها الهائلة (والتي قد تصل إلى 20 مليون يورو أو 4% من إجمالي الإيرادات السنوية العالمية، أيهما أعلى[1]) إلى تحويل الامتثال لحماية البيانات إلى مطلب أساسي للأعمال. وينتج عن ذلك أربع تحديات رئيسية:

الشكل 1. مخاطر حماية البيانات والآثار المترتبة عليها

[1] المادة 83 من اللائحة العامة لحماية البيانات.

شهادة الامتثال للائحة العامة لحماية البيانات (GDPR)

تسمح اللائحة العامة لحماية البيانات (GDPR) بالحصول على شهادة امتثال رسمية لمعالجة البيانات، والتي تهدف إلى *"إثبات امتثال عمليات المعالجة لهذه اللائحة من قبل المراقبين والمعالجين"* (المادة 42 من GDPR). كما تتيح *"لأصحاب البيانات بإجراء تقييم سريع لمستوى حماية البيانات الخاصة بالمنتجات والخدمات ذات الصلة"* (المادة 100 من GDPR). تُسهم هذه الشهادة أيضًا في تقليل المخاطر، بالإضافة إلى إثبات الامتثال التنظيمي وتعزيز قيمته.

قابلية تطبيق شهادة GDPR

لا يمكن تطبيق شهادة الامتثال للائحة العامة لحماية البيانات على الشركة ككل، بل يجب أن تركز على أنشطة معالجة بيانات محددة. يمكن لمقدمي الطلبات تحديد أنشطة معالجة البيانات ذات الأولوية للحصول على الشهادة وتحديد هدف واحد أو عدة أهداف للتقييم.

وبموجب GDPR، يمكن استخدام شهادة الامتثال من قِبل مراقبي ومعالجي البيانات، بما في ذلك:

- مقدمي الطلبات المتواجدين في المنطقة الاقتصادية الأوروبية والخاضعين للائحة وفقًا للمادة 3(1)؛
- مقدمي الطلبات المتواجدين خارج المنطقة الاقتصادية الأوروبية ولكنهم خاضعين للائحة وفقًا للمادة 3(2)؛
- مقدمي الطلبات المتواجدين خارج المنطقة الاقتصادية الأوروبية وغير الخاضعين مباشرةً للائحة ولكنهم يرغبون في إثبات امتثالهم بموجب المادة 46، ويشار إليهم غالباً باسم مستوردي البيانات (Data Importers).

تخضع معايير مقدمي الطلبات المتواجدين خارج المنطقة الاقتصادية الأوروبية حاليًا للمراجعة من قبل المجلس الأوروبي لحماية البيانات (EDPB). تكون الشهادات الممنوحة صالحة لفترات قابلة للتجديد مدتها ثلاث سنوات، مع إجراء عمليات تدقيق مراقبة سنوية.

القيمة القانونية لشهادة GDPR

على عكس معظم الشهادات، فإن **الشهادة الرسمية بموجب اللائحة العامة لحماية البيانات تُنتج آثارًا وتوفر مزايا قانونية للشركة الحاصلة عليها**. يمكن تصنيف منهجيات ومعايير التقييم إلى ثلاث فئات:

1. معايير مخصصة يتم إعدادها من قبل مسؤول حماية البيانات (DPO) أو من قبل الشركة نفسها.
2. معايير يتم وضعها من قبل منظمات تطوير المعايير، مثل ISO/IEC 27001 أو 27701.
3. معايير معترف بها رسميًا من قبل المجلس الأوروبي لحماية البيانات بموجب المادة 42 من اللائحة.

فقط الفئة الثالثة من المعايير يتم الاعتراف بها رسميًا وقانونيًا بموجب اللائحة العامة لحماية البيانات لإثبات الامتثال (المواد 24 و25 و28 و32) ولتقليل المخاطر.

شهادة GDPR مقابل الأدوات الأخرى

تعترف اللائحة العامة لحماية البيانات (GDPR) بعدة أدوات لدعم وإثبات الامتثال، إلا أن الشهادة تحتل موقعاً مميزاً ورئيسياً بينها:

الأثر التنظيمي وإثبات الامتثال

تُذكر الشهادة **في نص GDPR حوالي 73 مرة**، مقارنة بـ7 مرات فقط للبنود التعاقدية النموذجية (SCCs)، و36 مرة لمدونات قواعد السلوك (CC)، و25 مرة للقواعد المؤسسية الملزمة (BCRs). تم الاعتراف بالشهادة رسميًا في GDPR كوسيلة مناسبة لإثبات حماية البيانات بالتصميم (المادة 25 من GDPR)، والتزامات مراقب البيانات (المادة 24 من GDPR)، وامتثال معالج البيانات (المادة 28 من GDPR)، وأمن معالجة البيانات (المادة 32 من GDPR). كما يجب على القاضي أن يأخذ الشهادة بعين الاعتبار كعامل تخفيف عند تحديد قيمة الغرامة الإدارية (المادة 83 من GDPR).

الموثوقية

تُعتبر الشهادة أكثر موثوقية بدرجة كبيرة، حيث تعتمد على **عمليات تدقيق ومراقبة مستقلة تتم من خلال طرف ثالث**، على عكس الأدوات الأخرى مثل البنود التعاقدية النموذجية (SCCs). يعتمد مستوى الموثوقية على طبيعة الأدوات، فعلى سبيل المثال، تعتبر البنود التعاقدية النموذجية التزامًا قانونيًا من قبل كيان ما، ولكن لا يتم إجراء تدقيق ومراقبة لمدى الامتثال الفعلي وراءها. بينما تعتمد الشهادة على عمليات تدقيق منتظمة من جهات خارجية يقوم بها مدققون مؤهلون.

أما الأدوات الأخرى، مثل القواعد المؤسسية الملزمة والبنود التعاقدية، فهي تركز على السياسات العامة للشركة ولا تتحقق من الامتثال على مستوى عمليات معالجة البيانات نفسها، مما يترك مجالاً أكبر لعدم الامتثال. لتحديد مستوى الثقة في الامتثال الفعلي، يقوم مقياس مستوى الثقة والمعروف أيضًا باسم Trust Level Scale (TLS) بتوفير مقياسًا من A (موثوق للغاية) إلى I (غير موثوق على الإطلاق). عند تطبيق هذا المقياس على الأدوات الأربعة، تتفاوت النتيجة من الدرجة F بالنسبة للبنود التقاعدية النموذجية إلى درجة A بالنسبة للشهادة.

خلق القيمة

تحول الشهادة الامتثال إلى أصل غير ملموس ومصدر لخلق القيمة. تلعب جميع الأدوات دورًا في ضمان الامتثال، لكن الشهادة تتميز بقدرتها على تحويل الامتثال إلى أصل غير ملموس للشركة. وعلى غرار براءة الاختراع، تشكل الشهادة أصلاً غير ملموس للشركة، بحيث أنها تحول الامتثال إلى مصدر لخلق القيمة وتُستخدم كأداة قوية من قبل فرق التسويق والمبيعات لتمييز الشركة عن المنافسين. بالإضافة إلى ذلك، فهي تُسهم في بناء الثقة وتقليل الشكوك لدى المحللين الماليين والمستثمرين والمساهمين.

التوافر والوقت والجهد

تُعد معايير الشهادات والبنود التعاقدية النموذجية **أدوات معتمدة وجاهزة للاستخدام**، في حين تتطلب مدونات قواعد السلوك والقواعد المؤسسية الملزمة وقتًا وجهدًا كبيرين بالإضافة إلى التعاون بين الأطراف المعنية لتطويرها ووضعها قيد التنفيذ والموافقة عليها.
وعلاوة على ذلك، تُعتبر البنود التعاقدية النموذجية أكثر كفاءة في الحالات التي يكون فيها شريك تجاري واحد، حيث تتطلب التفاوض والاتفاق على الشروط مع كل شريك معني، في حين تُعد الشهادة أداة أكثر كفاءة في الحالات التي تشمل عدة شركاء، إذ تنطبق على عدد غير محدود من المراقبين والمعالجين.

الشمولية والمرونة والقدرة على التكيف

يمكن استخدام نفس المعايير عبر مختلف الصناعات (وهو ما لا ينطبق على مدونات قواعد السلوك) وعبر شركات متعددة (وهو ما لا ينطبق على القواعد المؤسسية الملزمة). على عكس الشهادات الأخرى التي قد تقتصر على معالجي البيانات فقط أو قد تكون محددة بهدف تقييم (Target of Evaluation) معين، فإن Europrivacy **لا تعتمد على قطاع محدد ويمكن استخدامها من قبل جميع مراقبي ومعالجي البيانات**. بالإضافة إلى ذلك، توفر Europrivacy المرونة والقابلية للتكيف، حيث تتيح للمؤسسات الفرصة **لتركيز جهودها على أنشطة معالجة البيانات ذات الأولوية لديها**.

هذان العنصران يجعلان Europrivacy متميزة عن الآليات الأخرى، مثل القواعد المؤسسية الملزمة المخصصة لشركة معينة ومدونات قواعد السلوك المخصصة لقطاع صناعي معين (مما يؤدي إلى خضوع المراقبين والمعالجين أحيانًا لمدونات سلوك مختلفة). كما أن كلًا من مدونات السلوك والقواعد المؤسسية الملزمة تركزان على متطلبات على مستوى الشركة بدلاً من أنشطة معالجة بيانات بحد ذاتها، مما يحد من قدرة المؤسسات على التركيز على احتياجاتها ذات الأولوية لحماية البيانات.

التوليف

يلخص الجدول التالي خصائص الشهادة مقارنة بالأدوات الثلاث الأخرى المتاحة للشركات.

	البنود التعاقدية النموذجية (SCC)	القواعد المؤسسية الملزمة (BCR)	مدونات قواعد السلوك (CC)	الشهادة
إثبات حماية البيانات بالتصميم وبشكل افتراضي بموجب المادة 25 من GDPR	لا	لا	لا	نعم
إثبات مدى كفاية مراقبي البيانات بموجب المادة 24 من GDPR	لا	لا	نعم	نعم
إثبات مدى كفاية معالجي البيانات بموجب المادة 28 من GDPR	لا	لا	نعم	نعم
كفاية أمن معالجة البيانات بموجب المادة 32 من GDPR	لا	لا	نعم	نعم
التأثير على الغرامات الإدارية بموجب المادة 83 من GDPR	لا	لا	نعم	نعم
الشمولية: قابلية التطبيق عبر مختلف الصناعات	نعم	لا	لا	نعم
وجود القيمة كأصل غير ملموس	لا	لا	لا	نعم
إمكانية التحديد والتركيز على معالجة البيانات ذات الأولوية	نعم	لا	لا	نعم
قابلية التوسع والتمديد (يمكن استخدام نفس النظام مع جميع شركاء B2B)	لا	نعم	نعم	نعم

الشكل 2. خصائص الأدوات المتعددة لـGDPR

كما هو موضح في الجدول، **تبرز الشهادة كأكثر الآليات** تأثيرًا، لما توفره من مزايا متعددة. ويؤكد ذلك أيضًا **عدد المرات** التي يتم فيها الإشارة رسميًا إلى كل أداة في نص GDPR (الشكل 3).

الأداة	عدد الإشارات الرسمية للأداة في GDPR	المادة	المراجع
البنود التعاقدية النموذجية	7	28, 57	81, 109, 168
القواعد المؤسسية الملزمة	25	4, 46, 47, 49, 57, 58, 64, 70	107, 108, 110, 168
مدونات قواعد السلوك	36	24, 28, 32, 35, 40, 41, 46, 57, 58, 64,70, 83	77, 81, 98, 99, 148, 168
الشهادة	73	24, 25, 28, 32, 42, 43, 46, 57, 58, 64, 70, 83	77, 81, 100, 166, 168

الشكل 3. الإشارات الرسمية إلى كل أداة في GDPR

Europrivacy

تمت الموافقة على Europrivacy من قبل المجلس الأوروبي لحماية البيانات (EDPB) والمنظمة الأوروبية للاعتماد (EA) لتكون بمثابة **الختم الأوروبي الرسمي لحماية البيانات** بموجب المادة 42 من اللائحة العامة لحماية البيانات (GDPR). تم **الاعتراف بـEuroprivacy رسميًا من قبل الاتحاد الأوروبي (EU) والمنطقة الاقتصادية الأوروبية (EEA) وسلطات حماية البيانات الوطنية الثلاثين التابعة لهما**. يمكن استخدام Europrivacy من قِبل كل من مراقبي ومعالجي البيانات للتصديق على جميع أنواع أنشطة معالجة البيانات. في الوقت الحالي، تقتصر شهادة GDPR على مقدمي الطلبات المقيمين في المنطقة الاقتصادية الأوروبية، ولكن من المتوقع أن يتم توسيع نطاقها قريباً ليشمل دولًا خارج المنطقة.

تم تطوير Europrivacy بالاستناد إلى المعيار الدولي ISO/IEC 17065 ويمكن دمجها بسهولة مع معايير ISO 27001 وISO 27701. في حال الجمع بينهما، يمكن تقصير عملية الشهادة حيث أن ISO/IEC 27001 معترف بها من قبل Europrivacy كمعادل لمجموعة فرعية من معاييرها.

تتضمن Europrivacy معايير متخصصة في مجالات وتقنيات محددة لضمان تقييم شامل وموثوق للامتثال. يجعل هذا الهيكل الفريد Europrivacy مناسبًا **لجميع أنواع أنشطة معالجة البيانات**، بما في ذلك تلك التي تتضمن **تقنيات ناشئة** مثل الذكاء الاصطناعي وإنترنت الأشياء وسلسلة الكتل والمعروفة بالبلوكتشين.

النشأة والتحديث المستمر

تم تطوير Europrivacy في إطار برنامج الأبحاث الأوروبي وبدعم مالي من المفوضية الأوروبية، ويُدار من قبل المركز الأوروبي للشهادات والخصوصية (ECCP) في لوكسمبورغ بإشراف مجلس خبراء دولي يتألف من مختصين في قانون حماية البيانات والأمن السيبراني وإصدار الشهادات والاعتماد. معًا، يقومون بمراقبة وتحديث نظام Europrivacy باستمرار لضمان توافقه مع أي تغييرات تنظيمية وتطورات اجتهادات قضائية.

منظومة شركاء Europrivacy

تحظى Europrivacy بدعم منظومة عالمية من الشركاء الذين يجب أن يثبتوا كفاءتهم وموثوقيتهم من خلال عملية اختيار. تضم هذه المنظومة العديد من الجهات العالمية الرائدة في مجالات الاستشارات القانونية وشركات المحاماة وجهات إصدار الشهادات ومزودي الحلول، إذ يضمنون معًا تغطية واسعة للسوق لدعم جميع الشركات المهتمة، بغض النظر عن موقعها الجغرافي، كما يمنعون مخاطر الاحتكار التجاري أو الأسعار غير العادلة.

امتدادات المعايير

يمكن تطبيق منهجية Europrivacy لتقييم واعتماد الامتثال التنظيمي مع تشريعات أوروبية أخرى أو تشريعات وطنية خارج الاتحاد الأوروبي من خلال ما يسمى بامتدادات المعايير (Criteria Extensions)، إذ يمكن استخدامها جنبًا إلى جنب مع معايير Europrivacy أو بشكل مستقل عنها للحصول على شهادة تكميلية. فيما يلي أمثلة على امتدادات معايير الاتحاد الأوروبي:

- معايير توجيه الخصوصية الإلكترونية (ePrivacy Directive) لتوجيه EC/58/2002 بشأن الخصوصية والاتصالات الإلكترونية.
- معايير قانون البيانات (Data Act) للائحة (EU) 2854/2023 بشأن القواعد الموحدة للوصول العادل إلى البيانات واستخدامها.
- معايير قانون حوكمة البيانات (Data Governance Act) للائحة (EU) 868/2022 بشأن الحوكمة الأوروبية للبيانات.
- معايير قانون المرونة التشغيلية الرقمية (DORA) للائحة (EU) 2554/2022 المتعلقة بالمرونة التشغيلية الرقمية للقطاع المالي.
- شهادة قانون الذكاء الاصطناعي (AI Act Cert) لتقييم الامتثال للائحة (EU) 1689/2024 المتعلقة بالقواعد الموحدة للذكاء الاصطناعي، ومبادئ منظمة التعاون الاقتصادي والتنمية (OECD) بشأن الذكاء الاصطناعي، والاتفاقية الإطارية لمجلس أوروبا بشأن الذكاء الاصطناعي وحقوق الإنسان والديمقراطية وسيادة القانون.

Interprivacy

Interprivacy هي النسخة الدولية لـEuroprivacy، إذ توفر **نظامًا دوليًا لشهادات حماية البيانات معتمدة من قبل المنتدى الدولي للاعتماد (IAF)** وسلطات الاعتماد التابعة له والبالغ عددها 95 سلطة في جميع أنحاء العالم، بما في ذلك الولايات المتحدة الأمريكية وكندا والبرازيل واليابان والمملكة المتحدة والهند. تتيح Interprivacy الفرصة لتقييم واعتماد الامتثال لمجموعة من أهم التشريعات العالمية لحماية البيانات الشخصية، مثل:

- اللائحة العامة لحماية البيانات (GDPR)
- اتفاقية حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية (اتفاقية 108+) لمجلس أوروبا
- إطار قواعد الخصوصية عبر الحدود (CBPR) وإطار الخصوصية لمنتدى التعاون الاقتصادي لآسيا والمحيط الهادي (APEC)
- إطار خصوصية البيانات بين الاتحاد الأوروبي والولايات المتحدة (DPF)
- إطار عمل رابطة دول جنوب شرق آسيا (ASEAN) لحماية البيانات
- معايير حماية البيانات الشخصية للدول الأيبيرية الأمريكية
- اتفاقية الاتحاد الإفريقي للأمن السيبراني وحماية البيانات الشخصية (اتفاقية مالابو)

رغم حيادها الجغرافي، فإن معايير ومنهجية Interprivacy تتماشى بشكل وثيق مع Europrivacy، مما يسهل قابلية التشغيل البيني والاعتراف المتبادل عبر الولايات القضائية المختلفة. كما أنها تمكّن المؤسسات من التحول بشكل سلس نحو شهادة GDPR الرسمية مع شهادة Europrivacy أو الجمع بين الشهادتين، لتبسيط جهود الامتثال.

الشكل 4. التغطية الجغرافية لمنتدى الاعتماد الدولي

لماذا: عرض قيمة Europrivacy

الشكل 5. عرض القيم

الحد من المخاطر

تمكّن شهادة Europrivacy من الحد من المخاطر التي يتعرض لها أصحاب البيانات والشركاء التجاريين والمتقدمين للشهادة، بما في ذلك المخاطر القانونية والمالية والمخاطر المتعلقة بالسمعة. تسمح المعايير المعتمدة من خلالها بالتحقق من الامتثال بطريقة منهجية وذلك بهدف تحديد وتصحيح أية حالات عدم امتثال محتملة. تساهم الشهادة أيضًا في التقليل بشكل مباشر من تقليل المسؤولية القانونية على مراقبي البيانات عند استخدام عمليات معالجة بيانات معتمدة.

توفير التكاليف

تسهم شهادة Europrivacy في تبسيط وتقليل تكاليف متطلبات العناية الواجبة والجهود المطلوبة بموجب المادة 28 من GDPR. كما أنها تقلل بشكل كبير من احتمالية الوقوع في مخالفات تنظيمية، وفي حالة حدوث خرق (مثل تسريب بيانات بعد هجوم إلكتروني)، يجب على القاضي أخذ الشهادة بعين الاعتبار وتخفيض مبلغ الغرامة. بشكل عام، يمكن استخدام شهادة Europrivacy لتبسيط وتوحيد إدارة الامتثال استنادًا إلى معايير معتمدة رسميًا.

تعزيز قيمة الامتثال

تمثل شهادة Europrivacy ميزة تنافسية ومصدرًا لتحقيق إيرادات إضافية، فهي تمكن المؤسسات من دخول أسواق جديدة والتفوق على المنافسين. كما تحول الامتثال إلى أصل جديد لمقدم الطلب وتغير منظور الامتثال من مركز تكلفة إلى مركز قيمة وربح. بشكل عام، تمكّن هذه الشهادة من تعزيز قيمة الجهد المستثمر في الامتثال داخليًا وخارجيًا، بالإضافة إلى المساهمة في رفع قيمة المؤسسة في السوق من خلال إظهار مستوى منخفض من المخاطر للمستثمرين والمساهمين.

بناء الثقة والسمعة الجيدة

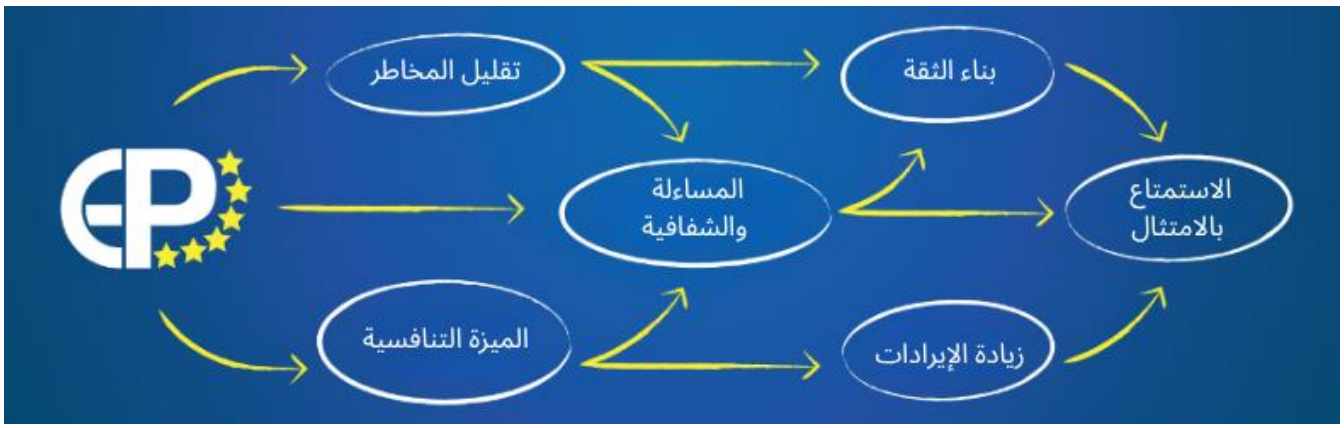
تُمكِّن شهادة Europrivacy من بناء الثقة من خلال إظهار الامتثال وتقليل المخاطر للأطراف الثالثة، مثل أصحاب البيانات والعملاء وشركاء الأعمال بين الشركات. كما تحظى Europrivacy بدعم وتأييد من كبرى شركات المحاماة والشركات الاستشارية وهيئات الاعتماد ومزودي الحلول، وهو ما يمثل أيضًا مصدرًا للثقة.

التبسيط

تسهم Europrivacy في توحيد وتبسيط إدارة الامتثال باستخدام معايير مشتركة من خلال معالجة البيانات والشركات والمواقع الجغرافية. نظرًا لإمكانية توسعها لتشمل لوائح تنظيمية أخرى وتكاملها مع حلول تقنية رئيسية (SAP، وOneTrust، وSGG، وغيرها)، فهي توفر أداة قوية لتبسيط وتوسيع نطاق إدارة الامتثال.

جعل الامتثال تجربة ممتعة

تم تطوير Europrivacy لتجعل من الامتثال أمرًا أبسط وأكثر متعة، فهي تقلل من الضبابية والتوتر الذي قد يشعر به مسؤول حماية البيانات (DPO) والشركة، كما تسهم في إضفاء قيمة على الامتثال وجعله معترفًا به. تقدم Europrivacy خدمات عبر الإنترنت، بما في ذلك التنبيهات في حال حدوث تغييرات تنظيمية، مما يبسط إدارة الامتثال بشكل كبير. إن Europrivacy أكثر بكثير من مجرد نظام إصدار شهادات، فهي تُمكِّن الشركات من الانضمام إلى مجتمع من الخبراء ومنظومة من الشركاء الموثوقين.



الشكل 6. عرض قيم Europrivacy

تفرّد Europrivacy

- **تم الاعتراف بـEuroprivacy رسميًا من قبل المجلس الأوروبي لحماية البيانات (EDPB) والمنظمة الأوروبية للاعتماد (EA)، في حين تم الاعتراف بـinterprivacy من قبل المنتدى الدولي للاعتماد (IAF). كلا النظامين متوافقان بشكل وثيق ويستخدمان معايير متشابهة يمكن تطبيقها في جميع أنحاء العالم.**
- تحظى Europrivacy بدعم **منظومة موثوقة تضم أكبر شركات المحاماة والشركات الاستشارية وهيئات الاعتماد ومزودي الحلول** في مجال الامتثال لحماية البيانات. وتضمن هذه المنظومة عدم احتكار الخدمة أو انقطاعها، مع توفير عروض عادلة ذات قيمة عالية مقابل التكلفة.
- **يمكن استخدام Europrivacy من قِبل مراقبي البيانات ومعالجيها على حد سواء لجميع أنواع معالجة البيانات، بما في ذلك معالجة البيانات المتعلقة بالتكنولوجيا مثل الذكاء الاصطناعي، وسلسلة الكتل (Blockchain)، والبيانات الاصطناعية، وإنترنت الأشياء.**
- تعتمد Europrivacy على عمليات تحقق ومراجعة شاملة بهدف الحد من المخاطر بشكل فعال لكل من مقدم الطلب للشهادة والشركاء التجاريين وأصحاب البيانات.
- **يمكن توسيع نطاق Europrivacy بسهولة ليشمل تشريعات بيانات أخرى، بما في ذلك قوانين الاتحاد الأوروبي واللوائح الوطنية.**
- يتم دعم Europrivacy بالأصل من قِبل مزودي حلول رئيسيين (مثل OneTrust وSAP وSGG وغيرها) لتبسيط وتسريع عملية إصدار الشهادة.

كيف: رحلة الحصول على الشهادة

تم تحسين رحلة الحصول على الشهادة لتكون بسيطة، فضلاً عن كونها فعالة من حيث الوقت والتكلفة:

يجب على مراقبي ومعالجي البيانات الخاضعين للائحة العامة لحماية البيانات (GDPR) الامتثال للتشريع على أي حال، إذ تركز الشهادة بشكل أساسي على تقييم هذا الامتثال وتوثيقه. ونتيجة لذلك، فإن معظم الجهد المطلوب من مقدم الطلب يكون قد اكتمل قبل بدء عملية التقدم للشهادة. بمجرد امتثال مقدم الطلب للالتزامات القانونية، تكون الخطوات التالية كما يلي:

1. **اختيار هدف التقييم**: يقوم مقدم الطلب باختيار معالجة البيانات ذات الأولوية وتحديد هدف التقييم المراد اعتماده.
2. **التحقق من الامتثال وتوثيقه للحد من المخاطر**: يقوم مقدم الطلب أو أحد الشركاء الرسميين بمراجعة وتوثيق امتثال أنشطة معالجة البيانات المختارة حسب معايير Europrivacy وInterprivacy. يساهم ذلك في التقليل من المخاطر التي يتعرض لها جميع الأطراف، بما في ذلك المخاطر القانونية والمالية والمخاطر المتعلقة بالسمعة لمقدم الطلب.
3. **الحصول على الشهادة لإثبات الامتثال**: يختار مقدم الطلب جهة إصدار شهادات متعمدة للتصديق وإثبات الامتثال، ويمكن استخدام النموذج الإلكتروني على موقع Europrivacy لتلقي العروض. يتم نشر الشهادات الصادرة في السجل الرسمي الذي يحتفظ به ECCP لتمكين التحقق من صحتها ومنع تزويرها.
4. **الحفاظ على الامتثال وتحويله إلى قيمة مضافة**: يمكن لمقدم الطلب بعد ذلك البدء في تحويل الامتثال إلى قيمة مضافة، فالشهادة تحول الامتثال إلى أصل غير ملموس يمكن استخدامه كميزة تنافسية ومصدر للعوائد.

الشكل 7. الرحلة الذكية للحصول على الشهادة

يتم دعم عملية الحصول على الشهادة من خلال مجموعة متكاملة من الموارد، بما في ذلك:

1. **منظومة Europrivacy العالمية من الشركاء الرسميين**، بما في ذلك منفّذ الامتثال (Implementer) للمساعدة في التحضير للشهادة، ومزودي الحلول لدعم توثيق الامتثال، وجهات إصدار الشهادات المعتمدة.
2. **أكاديمية Europrivacy الإلكترونية (Europrivacy Academy)** لتعلم كيفية استخدام وتطبيق معايير Europrivacy.
3. **المجتمع الالكتروني وموقع الموارد الرسمي لـEuroprivacy (Europrivacy Community and Resources)** حيث توجد جميع المعلومات والوثائق اللازمة، بما في ذلك النماذج والإرشادات والمنتدى وقسم متكامل للأسئلة الشائعة.

كما تقدم Europrivacy أيضاً باقة ترحيبية (Welcome Pack): توفر حزمة شاملة من المصادر والموارد لمقدم الطلب لمدة ثلاث

سنوات.

العائد على الاستثمار

الاستثمار

يعد الاستثمار المطلوب للحصول على شهادة Europrivacy محدود نسبيًا مقارنة بالجهد المطلوب للامتثال للائحة العامة لحماية البيانات (GDPR). وقد يختلف هذا الجهد حسب حجم وتعقيد هدف التقييم (Target of Evaluation). يمكن للمتقدم الاستفادة من الشركاء الرسميين الذين يمكنهم تولي قيادة عملية التحضير للشهادة وتوفير الحلول المناسبة لتوثيق الامتثال.

قد يتطلب استخدام الشركاء الرسميين ميزانية إضافية، ولكنه سيقلل من الوقت والجهد اللازمين لمقدم الطلب. يحدد الشركاء الرسميون الرسوم الخاصة بهم، والتي قد تختلف وفقًا لبلد التشغيل.

بمجرد توثيق الهدف الأول للتقييم، يمكن إعادة استخدام جزء من هذا التوثيق في الشهادات المستقبلية. نتيجةً لذلك، تتطلب الشهادات اللاحقة لأنشطة معالجة بيانات إضافية وقتًا وجهدًا أقل من الشهادة الأولى.

عند الانتهاء من الشهادة، تقوم جهة إصدار الشهادة بنشرها في **السجل الرسمي لشهادات Europrivacy**، وهو ما يترتب عليه رسوم إضافية. إذا كان مقدم الطلب قد قام بشراء باقة ترحيبية، فإنها تغطي رسوم النشر لأول شهادتين.

التكاليف الإلزامية

1. تكاليف التدقيق من قبل **جهة إصدار الشهادة.**
2. **رسوم النشر في السجل الرسمي** (عادةً ما تكون مشمولة في عرض جهة إصدار الشهادة): يجب نشر شهادات Europrivacy الصادرة في السجل الرسمي لتصبح سارية المفعول. يعالج هذا السجل متطلبات المجلس الأوروبي لحماية البيانات (EDPB) فيما يتعلق بالشفافية ويمكّن الأطراف الثالثة من التحقق من صحة الشهادات الصادرة ومنع تزويرها. يتم تغطية رسوم النشر للمرة الأولى والثانية ضمن الباقة الترحيبية.

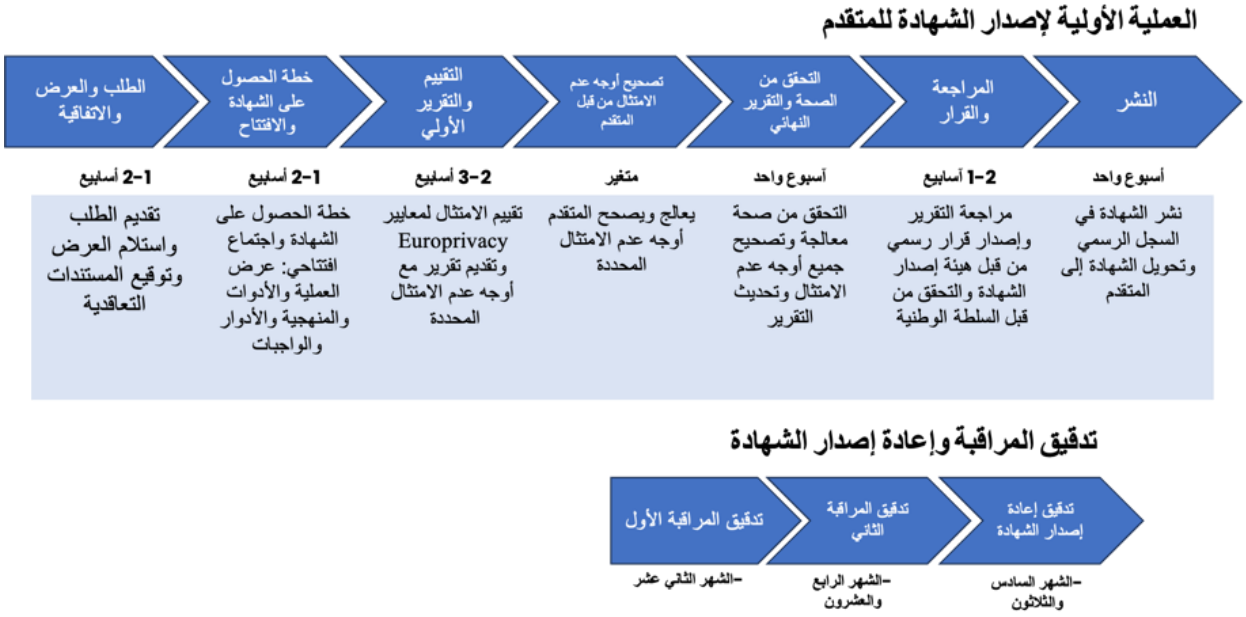
التكاليف الاختيارية

1. **الباقة الترحيبية:** توفر الباقة الترحيبية مجموعة كاملة من الموارد للمتقدم لمدة ثلاث سنوات. تبلغ قيمتها 6,000 يورو وغالبًا ما تكون مشمولة ضمن عرض خدمة المنفذ (Implementer).
2. **رسوم المنفذ:** إذا قام مقدم الطلب بتفويض التحضير للشهادة إلى منفذ مؤهل، فإنه تطبق رسوم إضافية. يمكن العثور على قائمة الشركاء الرسميين على موقع Europrivacy الإلكتروني.
3. **الحلول البرمجية**: يمكن لمقدم الطلب استخدام أحد مزودي الحلول لتسريع عملية توثيق الامتثال ودعمها.
4. **أكاديمية Europrivacy الإلكترونية (Europrivacy Academy):** يُنصح مقدمو الطلبات الراغبون في التحضير للشهادة بأنفسهم بإكمال دورة التنفيذ (Implementation Course) على موقع أكاديمية Europrivacy الإلكترونية، حيث تكون الدورة التمهيدية (Introductory Course) للأكاديمية مشمولة في الباقة الترحيبية.
5. **موقع مجتمع وموارد Europrivacy (Europrivacy Community and Resources):** يُنصح مقدمو الطلبات الراغبون في التحضير للشهادة بأنفسهم بالاشتراك في موقع مجتمع وموارد Europrivacy، إذ تغطي الباقة الترحيبية الاشتراك لمدة ثلاث سنوات.

كتوصية عامة، تعد الباقة الترحيبية خيارًا ذو قيمة عالية مقابل التكلفة، فهي تتيح الوصول إلى أهم الموارد اللازمة للحصول على الشهادة.

الوقت

يعتمد الوقت اللازم للحصول على شهادة Europrivacy على مستوى امتثال المؤسسة واستعدادها لاستخدام الموارد الخارجية مثل المنفذين المؤهلين أو مزودي الحلول. بشكل عام، إذا كانت معالجة البيانات متوافقة مع اللائحة العامة لحماية البيانات (GDPR)، يمكن إعداد وثائق الامتثال بسرعة، خاصة عند الاستعانة بمنفذين مؤهلين.



الشكل 8. مثال على الجدول الزمني لعملية الحصول على الشهادة

قيمة الشهادة

يعتبر الحصول على شهادة Europrivacy استثمارًا استراتيجيًا وليس مجرد تكلفة، حيث يحول الامتثال إلى مصدر يولّد قيمة ويحقق عوائد ملموسة:

1. **تشكل ميزة تنافسية** في السوق يمكن استخدامها من قبل فرق التسويق والمبيعات لزيادة إيرادات المتقدم.
2. **تتيح فرصًا جديدة في السوق** التي تعد شهادة الامتثال شرطًا أساسيًا فيها.
3. **تساهم في تقليل تكاليف العناية الواجبة** لكل من مراقبي ومعالجي البيانات بموجب المادة 28 من اللائحة العامة لحماية البيانات (GDPR).
4. **تُظهر انخفاض المخاطر القانونية والمالية للمساهمين**، مما يؤدي إلى تقييم أعلى في السوق المالي.
5. **تبني الثقة لدى المستثمرين المحتملين**.
6. **تقلل من المخاطر القانونية والمالية**. يوفر موقع Europrivacy الإلكتروني حاسبة توفير التكاليف حسب اللائحة العامة لحماية البيانات (GDPR) لتقييم التوفير المحتمل في التكاليف بفضل اعتماد شهادة الامتثال مع التركيز على التكاليف الخفية المرتبطة بالمخاطر القانونية والمالية.
7. **تتيح تبسيط إدارة الامتثال** باستخدام المتطلبات القياسية استنادًا إلى المعايير المعتمدة رسميًا من قبل المجلس الأوروبي لحماية البيانات (EDPB) وسلطاته الوطنية الثلاثين.

قالوا عنّا

فيليب رايثر، المسؤول الرئيسي عن الخصوصية في مجموعة Allianz

"هناك فائدة خارجية وأخرى داخلية لشهادة Europrivacy. من منظور داخلي، هي عملية لإدارة المخاطر يتم فيها تحديد الثغرات ومعالجتها والتحسن من خلالها. أما بالنسبة للفوائد الخارجية، فإنك تُظهر للعملاء والموظفين والمستثمرين أن البيانات آمنة هنا، وهذا مثبت من خلال ختم حماية البيانات الأوروبي، مما يزيد من ثقة أصحاب المصلحة في مؤسستك وفي طريقة تعاملك مع البيانات."

سيدريك نيديليك، مسؤول حماية البيانات (DPO) في PwC لوكسمبورغ

"تحدد اللائحة العامة لحماية البيانات (GDPR) المبادئ والأهداف ولكنها لا توفر الوسائل اللازمة لتحقيقها. لقد أثارت شهادة Europrivacy بعض الأسئلة، وقدمت زوايا متعددة لحماية البيانات، وجعلتنا نفكر بشكل مختلف، كما أنها تمكننا ماديًا من أن نكون أكثر كفاءة من الناحية التشغيلية. الحقيقة أننا قادرون الآن على الإشارة رسميًا إلى أن طرفًا ثالثًا مستقلًا قد اعتبر منصتنا متوافقة مع مجموعة من الضوابط المختلفة، وهو ما يضيف قيمة حقيقية أمام العملاء وأصحاب المصلحة."

دافيدي روفو، رئيس العلاقات المؤسسية في AINDO

"إن شهادة Europrivacy تقلل من مخاطرنا بشكل كبير، وتخفض احتمالية حدوث انتهاكات للبيانات وعقوبات عدم الامتثال، مما يجعلها أداة قوية لبناء الثقة مع عملائنا وشركائنا وأصحاب المصلحة. كما أنها تعمل كوسيلة حماية داخلية وتعزز أيضاً من ثقة العملاء كمصدر أمان إضافي. فهي لا تثبت جهودنا في الامتثال فحسب، بل تعزز أيضًا من سمعتنا كمؤسسة مسؤولة وجديرة بالثقة، وتسهم في نشر ثقافة الامتثال داخل مؤسستنا من خلال تثقيف الفريق وتدريبه."

لويس ماري غريف، مسؤول الأخلاقيات الرقمية في Piano

"إن الحصول على شهادة Europrivacy يعكس الجهد العميق الذي بذله فريقنا لإدماج مبادئ الخصوصية والأخلاقيات والامتثال حسب التصميم في أساس Piano Analytics. يؤكد اجتياز التدقيق بموجب نظام Europrivacy أن هذه المبادئ ليست مجرد طموحات، بل إنها ممارسات عملية. وهذا اعتراف نفخر بمشاركته مع عملائنا وشركائنا."

جيوفاني فرانشيسكوتي، رئيس تمكين المبيعات العالمية في DNV، وهي هيئة اعتماد عالمية معترف بها كشريك رسمي لـEuroprivacy:

"لقد استجابت Europrivacy لجميع احتياجاتنا، فهي منظمة بشكل جيد لتقييم الأطراف الثالثة ولكن أيضًا لتنفيذ الضوابط، كما أن فريق خبراء ECCP يُحدث الفرق عندما يتعلق الأمر بتطبيق النظام. يُعتبر الختم دليلًا على أن الشركة تخفف من المخاطر وتركز على ما هو مهم حقًا – حقوق واحتياجات أصحاب البيانات – بينما تقدم في الوقت نفسه إجابة فعلية للسوق. نصيحتي للمهتمين بالحصول على الشهادة هي عدم الخوف من العملية وإشراك جهات إصدار الشهادة وجميع خبراء منظومة Europrivacy منذ البداية."

هيا بنا!

الإجراءات المقترحة

للاستعداد بنجاح للحصول على شهادة Europrivacy، ينبغي على المؤسسات النظر في الخطوات التالية:

1. **الالتزام بحماية البيانات الشخصية** من خلال التسجيل في **ميثاق الخصوصية (Privacy Pact)**.
2. **تعيين مسؤول حماية بيانات (DPO)** يمكن الوصول إليه بسهولة من قبل العامة والسلطة الإشرافية الوطنية.
3. **توثيق أنشطة معالجة البيانات** وضمان **قانونيتها وتقليل البيانات المعالجة إلى الحد الأدنى**.
4. **تقييم المخاطر المحتملة** على حقوق وحريات أصحاب البيانات، وإذا لزم الأمر، إجراء تقييم أثر حماية البيانات (DPIA).
5. تنفيذ **تدابير تكنولوجية وتنظيمية** لمنع الوصول غير المصرح به إلى البيانات أو الكشف عنها أو فقدانها. يجب مراجعة هذه التدابير بانتظام وتحديث تقييم المخاطر عند الحاجة.
6. **إبلاغ واعتماد سياسة وقواعد وإجراءات حماية البيانات**، بما في ذلك التحكم في الوصول، والنسخ الاحتياطي، وفترة الاحتفاظ بالبيانات، وحقوق أصحاب البيانات، والمعالجين، ونقل البيانات الشخصية عبر الحدود.
7. تسجيل وتوثيق **ممارسة حقوق أصحاب** البيانات، وكذلك أي **انتهاكات للبيانات والإجراءات المتخذة للتخفيف من حدتها.**
8. **إعداد المراجعات السنوية من قبل الإدارة العليا** ووضع خطط العمل.

جهات الاتصال

للحصول على المزيد من الإرشادات، يمكنك زيارة الموقع الإلكتروني europrivacy.org، حيث يمكنك العثور على معلومات شاملة حول Europrivacy وطلب عروض أسعار للخدمات من خلال نموذج طلب عروض أسعار الخدمات.

كما يمكنك التواصل معنا للحصول على الدعم والإرشاد عبر البريد الإلكتروني contact@europrivacy.com.

إذا كنت مستعدًا لبدء رحلتك للحصول على شهادة Europrivacy، فلا تتردد في الحصول على باقة ترحيبية و/أو الانضمام إلى موقع مجتمع Europrivacy للاستفادة من الأدوات والموارد القيّمة والدعم من الخبراء.

مصادر مفيدة

المصادر الإلكترونية

موقع Europrivacy الإلكتروني: يوفر معلومات عامة عن Europrivacy، بما في ذلك المعايير، وقائمة الشركاء الرسميين، وآلة حاسبة لتقدير التكاليف التي يمكن لمقدم الطلب توفيرها من خلال الحصول على الشهادة.

أكاديمية Europrivacy الإلكترونية (Europrivacy Academy): تمكّن من التعرف على Europrivacy، وتعلم كيفية تطبيقه، والحصول على مؤهلات رسمية كمنفذ (Implementer) أو مدقق (Auditor).

موقع مجتمع وموارد Europrivacy: يتيح الوصول إلى جميع الوثائق المطلوبة، بما في ذلك المعايير والنماذج والمبادئ التوجيهية، لتوثيق الامتثال وإعداد الشهادة.

منظومة الشركاء الرسميين

يتم تحديث قائمة الشركاء الرسميين على موقع Europrivacy الإلكتروني. يمكنك طلب عرض من شركاء Europrivacy الرسميين عبر الإنترنت من خلال الرابط: https://www.europrivacy.com/en/apply

الباقة الترحيبية

الباقة الترحيبية هي حزمة خدمات صالحة لمدة ثلاث سنوات لدعم مقدم الطلب، وتشمل:

- **ساعة واحدة من الدعم والتوجيه الشخصي عبر الإنترنت**
- **المساعدة في العثور على منفذين أو مزودي حلول أو جهات إصدار الشهادات**
- **دورة تمهيدية واحدة (Introductory Course) لمسؤول حماية البيانات (DPO)**
- **الوصول إلى موارد Europrivacy عبر الإنترنت لمدة ثلاث سنوات**
- **تنبيهات Europrivacy الفورية حول التحديثات التنظيمية** لتبقى على اطلاع دائم بالتغييرات، والأحكام القضائية، ومنشورات المجلس الأوروبي لحماية البيانات (EDPB)، وغيرها
- **ميثاق خصوصية واحد (Privacy Pact) لإظهار الالتزام باحترام حماية البيانات واللائحة العامة لحماية البيانات (GDPR)**
- **رسوم نشر أول شهادتين لـEuroprivacy في السجل الرسمي**
- **الوصول إلى منظومة Europrivacy** والشركاء المعتمدين والخبراء والشركات المؤهلة

الرابط: https://www.europrivacy.com/en/welcomepack

الاتصال بـEuroprivacy

يمكن للمتقدمين المهتمين الاتصال مع المركز الأوروبي للشهادات والخصوصية (ECCP) للحصول على المعلومات والإرشاد من خلال نموذج الاتصال التالي: https://www.europrivacy.com/en/contact/contact-us

روابط مفيدة

- موقع Europrivacy الرسمي: www.europrivacy.com بما في ذلك أداة حساب التوفير من خلال شهادة GDPR: https://www.europrivacy.org/en/resource/gdpr-estimator
- أكاديمية Europrivacy: https://academy.europrivacy.com/
- مجتمع وموارد Europrivacy: https://eccpcenter.org
- موقع Interprivacy الرسمي: www.interprivacy.com
- ميثاق الخصوصية (Privacy Pact): https://www.privacypact.com
- الموقع الرسمي للمركز الأوروبي للشهادات والخصوصية (ECCP): https://eccpcenter.org/
- سجل شهادات المركز الأوروبي للشهادات والخصوصية: https://repository.europrivacy.org/en/certifications/search
- الموقع الرسمي للمجلس الأوروبي لحماية البيانات (EDPB): https://www.edpb.europa.eu/edpb_en

التعريفات

المصطلح	التعريف
مقدم الطلب (Applicant)	العميل الذي يتقدم بطلب للحصول على شهادة Europrivacy لدى جهة إصدار الشهادات.
مراقب البيانات (Data Controller)	الكيان الذي يحدد أغراض ووسائل معالجة البيانات الشخصية، سواء بشكل منفرد أو بالاشتراك مع جهات أخرى (المادة 4 (7) من اللائحة العامة لحماية البيانات GDPR).
معالجة البيانات (Data Processing)	أي عملية يتم إجراؤها على البيانات الشخصية، بما في ذلك جمع البيانات الشخصية أو تسجيلها أو تنظيمها أو تخزينها أو تغييرها أو استرجاعها أو الاطلاع عليها أو استخدامها أو الإفصاح عنها أو حجبها أو محوها أو إتلافها (المادة 4 (2) من اللائحة العامة لحماية البيانات GDPR).
معالج البيانات (Data Processor)	الكيان الذي يقوم بمعالجة البيانات الشخصية نيابةً عن مراقب البيانات (المادة 4 (8) من اللائحة العامة لحماية البيانات GDPR).
صاحب البيانات (Data Subject)	شخص طبيعي محدد أو قابل للتحديد تتم معالجة بياناته الشخصية (المادة 4 (1) من اللائحة العامة لحماية البيانات GDPR).
المجلس الأوروبي لحماية البيانات (EDPB)	هيئة مستقلة تضمن التطبيق الموحد للائحة العامة لحماية البيانات (GDPR) في جميع أنحاء الاتحاد الأوروبي وتعزز التعاون بين السلطات الوطنية لحماية البيانات.
البيانات الشخصية (Personal Data)	أي معلومات تتعلق بصاحب البيانات، مثل الاسم، أو رقم التعريف، أو بيانات الموقع الجغرافي، أو المُعرّف الإلكتروني، أو عامل واحد أو أكثر من العوامل الخاصة بالهوية البدنية أو الفسيولوجية أو الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لذلك الشخص (المادة 4 (1) من اللائحة العامة لحماية البيانات GDPR).
مالك نظام الشهادات (Scheme Owner)	المنظمة المسؤولة عن تطوير نظام شهادة Europrivacy وتحديثه.
السلطة الإشرافية (Supervisory Authority)	سلطة عامة مستقلة أنشأتها كل دولة عضو في الاتحاد الأوروبي لمراقبة تطبيق قوانين حماية البيانات، وفرض الامتثال للائحة العامة لحماية البيانات، وحماية حقوق الأفراد المتعلقة ببياناتهم الشخصية. (المادة 51 من اللائحة العامة لحماية البيانات GDPR)
هدف التقييم (Target of Evaluation)	وصف وتحديد أنشطة معالجة البيانات التي سيتم تقييمها واعتمادها من خلال عملية الشهادة. يجب أن يكون هدف التقييم محددًا بوضوح ويسهل فهمه من قبل أصحاب البيانات.

المركز الأوروبي للشهادات والخصوصية
20 شارع يوجين روبيرت
لوكسمبورغ L–2453 لوكسمبورغ
www.eccpcenter.org
www.europrivacy.com