اتفاقية من مراقب البيانات إلى معالج البيانات

وفقًا للمادة 28 من اللائحة الأوروبية العامة لحماية البيانات[1] (**GDPR**))

تشكل اتفاقية معالجة البيانات القائمة جزءًا لا يتجزأ من اتفاقية ترخيص المستخدم النهائي من Kaspersky ("اتفاقية الترخيص") بشأن توفير منصةKaspersky Adaptive Online Training Platform ("المنتج") بين:

*Kaspersky Lab Switzerland GmbH,*
*الواقعة في العنوان:[2] Bahnhofstrasse 100, 8001 Zürich, Switzerland*

-المعالج-

و

*العميل*

-المراقب-

القسم 1 غرض الاتفاقية ومدتها

1. غرض الاتفاقية

غرض هذه الاتفاقية منصوص عليه في اتفاقية الترخيص المكتوبة.

2. مدة الاتفاقية

مدة هذه الاتفاقية منصوص عليها في اتفاقية الترخيص المكتوبة.

القسم 2 نطاق معالجة البيانات وطريقتها وغرضها، وأنواع البيانات وتصنيفات أصحاب البيانات، وحقوق المراقب والتزاماته

1. طريقة معالجة البيانات وغرضها

غرض أنشطة المعالج منصوص عليه في اتفاقية الترخيص.

2. أنواع البيانات

أنواع البيانات الشخصية هي:

- معرّف الشركة (إن تم تقديمه)
- الاسم الأول والأخير
- البريد الإلكتروني
- بيانات التعريف التنظيمية (كما يتم تقديمها من مراقب البيانات)، بما يشمل:
  - القسم
  - المدير
  - الموظفين
- الإجراءات المسجلة داخل النظام خلال الاستخدام العادي، بما يشمل:

[1] اللائحة (الخاصة بالاتحاد الأوروبي) 679/2016 الصادرة من البرلمان الأوروبي ومن المجلس بتاريخ 27 أبريل 2016 بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة البيانات المذكورة، وإبطال التوجيه EC/46/95 (اللائحة العامة لحماية البيانات).

[2] يتم تطبيق تعريفات اللائحة العامة لحماية البيانات.

- المحتوى المُطلَع عليه
- البيانات المُعطاة
- الوقت المستغرق
- درجات التقييم الذاتي
- درجة الإكمال
- التعليقات والتعقيبات
- المحتوى المُنشأ

3. تصنيفات أصحاب البيانات

تصنيفات أصحاب البيانات هي:

(أ) موظفو مراقب البيانات العاملين مع المنصة أو المنتجين للمحتوى أو المتعلمين أو الحاصلين على معلومات حول التعلم أو جميع ما سبق.

(ب) عملاء مراقب البيانات الذين اشتروا حق الوصول إلى المنصة من خلال مراقب البيانات.

(ج) عملاء مراقب البيانات الذين اشتروا حق الوصول إلى المنصة من خلال معالج البيانات.

القسم 3 حق المراقب في إعطاء التعليمات

لا يجوز للمعالج معالجة البيانات الشخصية إلا بتعليمات موثقة من المراقب، بما يشمل ما يتعلق بنقل البيانات الشخصية لبلد أو منظمة دولية أخرى، ما لم يكن فعل ذلك مطلوبًا بقوانين الاتحاد أو دولة عضو فيه يخضع المعالج لها. في هذه الحالة، يجب على المعالج إبلاغ المراقب بهذه الضرورة القانونية قبل المعالجة، ما لم يكن القانون يحظر مثل هذه المعلومات لأسباب هامة للمصلحة العامة.

يجب على المعالج أن يصدر جميع التعليمات بصيغة مكتوبة (بالبريد الإلكتروني مثلًا). إن صدرت التعليمات شفهيًا على سبيل الاستثناء، فيجب تأكيدها بشكل مناسب بصيغة مكتوبة (بالبريد الإلكتروني مثلًا) من جانب المراقب.

يجب على المعالج أن يبلغ المراقب فورًا إن كانت إحدى التعليمات، في رأيه، تنتهك النظام الأوروبي العام لحماية البيانات (GDPR) أو أي من أحكام حماية البيانات الأخرى التي تخص الاتحاد او دولة عضو فيه.

القسم 4 الالتزام بالسرية/الالتزام بالحفاظ على السرية

يتأكد المعالج من أن الأشخاص المصرح لهم بمعالجة البيانات الشخصية ملتزمين بالسرية أو يخضعون لالتزام قانوني مناسب بالسرية.

القسم 5 أمن المعالجة/التدابير التنظيمية والفنية وفقًا للمادة 32 من النظام العام لحماية البيانات

يجب على المعالج أن يتخذ جميع التدابير التنظيمية والفنية الضرورية وفقًا للمادة 32 من النظام الأوروبي العام لحماية البيانات. وهي مذكورة بالتفصيل في الملحق 1.

التدابير الفنية والتنظيمية مرهونة بالتقدم والتطور التكنولوجيين. لمدة هذه الاتفاقية، يجب تعديل التدابير الفنية والتنظيمية المتخذة باستمرار حسب متطلبات الاتفاقية ويجب أن يقوم المعالج بمزيد من التطوير لها مع مراعاة هذه الاتفاقية والتقدم التكنولوجي. يجب ألا يقل مستوى الحماية عن التدابير الفنية والأمنية المذكورة في هذ الوثيقة وفي الملحق 1.

يوافق المعالج على توثيق التغييرات الكبيرة على التدابير الفنية والتنظيمية التي يكون لها أثر كبير على مستوى السلامة المضمون وذلك كتابيًا كإضافة للملحق 1 وأن يبلغ المراقب بأي مما سبق؛ ويجب أن يتم التوثيق المذكور بصورة إلكترونية أيضًا.

القسم 6 الاشتراك مع معالج آخر

قد يقوم المعالج بإشراك معالجين آخرين. أي معالج آخر مشترك في وقت الاتفاقية يجري النص عليه في الملحق 2 من هذه الاتفاقية. يجب على المعالج أن يبلغ المراقب كتابيًا، بما يشمل إبلاغه بصيغة إلكترونية، عن أي تغييرات مزمعة فيما يتعلق بإضافة معالجين آخرين أو استبدالهم. يتمتع المراقب بفرصة معارضة التغييرات المذكورة.

إن قام المعالج بإشراك معالج آخر لتنفيذ نشاطات معالجة نوعية بالنيابة عن المراقب، فإن جميع التزامات حماية البيانات عينها المنصوص عليها في العقد أو غيره من المواثيق القانونية بين المراقب والمعالج حسب المشار إليها في هذه الاتفاقية تُفرض على المعالج المذكور بطريق العقد أو غيره من المواثيق القانونية بموجب قوانين الاتحاد أو دولة عضو فيه، لا سيما فيما يتعلق بتقديم ضمانات كافية لتطبيق التدابير الفنية والتنظيمية بطريقة تجعل المعالجة تلبي متطلبات النظام الأوروبي العام لحماية البيانات. إن تخلف المعالج الآخر المذكور عن الوفاء بالتزاماته لحماية البيانات، يظل المعالج الأصلي مسؤولًا بالكامل أمام المراقب عن أداء التزامات المعالج الآخر المذكور.

القسم 7 واجب التعاون/واجب تقديم المساعدة

بالنظر إلى طبيعة المعالجة، يساعد المعالج المراقب بالتدابير الفنية والتنظيمية المناسبة، بقدر ما يمكن، للوفاء بالتزام المراقب بالاستجابة للطلبات التي تخص ممارسة أصحاب البيانات لحقوقهم والمنصوص عليها في الفصل الثالث من النظام الأوروبي العام لحماية البيانات (مع الأخذ في الحسبان حقوق أصحاب البيانات فيما يتعلق بالشفافية والحق في التمتع بإمكانية الوصول والحق في التصحيح والحق في المحو ("الحق في النسيان") والحق في تقييد المعالجة والالتزام بالإشعار فيما يتعلق بتصحيح البيانات الشخصية أو محوها أو تقييد المعالجة والحق في تحويل البيانات والحق في الاعتراض والحق في اتخاذ القرارات الفردية المشغلة آليًا).

القسم 8 الدعم في الوفاء بالتزامات مراقب البيانات

يساعد المعالج المراقب في ضمان تحقيق التزاماته بموجب المواد من 32 إلى 36 مع الأخذ في الحسبان طبيعة المعالجة والمعلومات المتوفرة للمعالج (ضمان أمن المعالجة؛ وإخطار السلطات المسؤولة عن خروقات البيانات الشخصية؛ وإبلاغ خروقات البيانات الشخصية لأصحاب البيانات؛ وتقييم تأثر حماية البيانات؛ والتشاور المسبق).

القسم 9 حذف البيانات الشخصية وإرجاعها

ما لم تُطبق فترات حفظ قانونية أو غير ذلك، يجب على معالج البيانات المتابعة بتنفيذ المذكور تاليًا بعد اكتمال الاتفاقية: عند طلب العميل، يجب على معالج البيانات تسليم البيانات الشخصية إلى المراقب بصيغة مقروءة وقابلة للتحرير وحذف النسخ الموجودة، ما لم يطلب المراقب من المعالج حذف البيانات الشخصية.

في حال عدم تلقي طلبات من المراقب، فسوف تُحذف البيانات الشخصية بعد مرور 90 يومًا من نهاية العقد مع العميل.

القسم 10 الإثبات بالالتزامات والدعم في التفتيش

يوفر المعالج للمراقب جميع المعلومات الضرورية التي تثبت الامتثال بالالتزامات المنصوص عليها في المادة 28 من النظام الأوروبي العام لحماية البيانات. ويسمح بعمليات التدقيق ويساهم بها، بما يشمل عمليات التفتيش، التي ينفذها المراقب أو مُدقق آخر مفوض من قبل المراقب.

القسم 11 متفرقات

إن تعرض الوفاء بغرض هذه الاتفاقية حسب المنصوص عليه في القسم 1 من هذه الاتفاقية من جانب المعالج للخطر نتيجة للحجز أو المصادرة أو الإعسار أو إجراءات التسوية القانونية أو نتيجة لغيرها من الأحداث والتدابير المتخذة من طرف الغير، فيجب على المعالج أن يبلغ المراقب فورًا. يجب على المعالج أن يبلغ جميع الأطراف المنخرطة بأن الحق في التصرف في البيانات يقع في يد المراقب وحده.

في حال وجود تعارض محتمل بين هذه الاتفاقية واتفاقية الترخيص فإن أحكام الاتفاقية القائمة تكون لها الأولوية على أحكام اتفاقية الترخيص.

تخضع هذه الاتفاقية لقانون الدولة العضو بالاتحاد الأوروبي المتواجد بها مراقب البيانات.

في حال بطلان أجزاء مفردة من هذه الاتفاقية، فيجب ألا يؤثر هذا على صلاحية بقية أجزاء الاتفاقية.

أي تعديل لهذه الاتفاقية، بما يشمل إنهاءها وأي تعديل على هذه البند، يجب أن يكون مكتوبًا؛ ويشمل المصطلح "مكتوبًا"الصيغة الإلكترونية أيضًا.

[المكان]، في [التاريخ] [المكان ]، في [التاريخ].

_____ _____

- المعالج - - المراقب-

الملحق 1 التدابير الفنية والتنظيمية وفقًا للمادة 32 من النظام الأوروبي العام لحماية البيانات

الملحق 2 المعالجون الآخرون

الملحق 1

التدابير الفنية والتنظيمية وفقًا للمادة 32 من النظام الأوروبي العام لحماية البيانات

بالنظر إلى

- الحالة الفنية
- وتكاليف التنفيذ
- وطبيعة ونطاق وسياق
- وأغراض المعالجة فضلًا عن
- خطر تفاوت احتمالية وخطورة حقوق الأفراد الطبيعيين وحرياتهم،

فيجب على المعالج أن يتخذ تدابير فنية وتنظيمية ملائمة لضمان مستوى الأمن المناسب لهذا الخطر.

وعند تقييم المستوى المناسب من الأمان، يجب أن وضع المخاطر المتعلقة بالمعالجة على وجه الخصوص في الحسبان، ولا سيما خطر التدمير العرضي أو غير القانوني والخسارة والتعديل والكشف غير المصرح به أو الوصول إلى بيانات شخصية منقولة أو مخزنة أو معالجة بطريقة بخلاف ذلك.

يتخذ المعالج التدابير الآتية:

تنظيم الأمن المعلوماتي

- يجرى تعيين مسؤول أمني أو أكثر مسؤولين عن تنسيق القواعد والإجراءات الأمنية ومراقبتها.
- يخضع الموظفون الأفراد ممن يصلون إلى بيانات العميل لالتزامات بالسرية.
- جرى تنفيذ تقييم مخاطر قبل معالجة البيانات الشخصية أو الشروع في الخدمات.

إدارة الأصول

- المحافظة على جرد لجميع الأصول (المخزنة فيها وبها البيانات الشخصية). الوصول إلى جرد هذه الوسائط مقصور على الموظفين المخولين للحصول على حق الوصول المذكور.
- البيانات الشخصية مصنفة للمساعدة في تحديدها والسماح بتقييد الوصول إليها بطريقة ملائمة.
- يجب الحصول على تفويض خاص قبل تخزين البيانات الشخصية في أجهزة منقولة أو معالجة البيانات الشخصية عن بعد أو معالجة البيانات الشخصية خارج منشآت الشركة.

أمن الموارد البشرية

- تبلغ الشركة موظفيها عن الإجراءات الأمنية ذات الصلة وأدوارهم المنوطة بهم.
- وكذلك تبلغ الشركة موظفيها بالعواقب الممكنة لخرق قواعد الأمن وإجراءاته
- تُجري الشركة تدريبات على أمن البيانات الشخصية

الأمن المادي والبيئي

- تُقيد الشركة الوصول إلى المنشآت التي توجد بها أنظمة المعلومات التي تعالج البيانات الشخصية ليقتصر على أشخاص مخولين محددين:
  - حرس أمني يقدمون خدمة الأمن على مدار الساعة طوال أيام الأسبوع
  - التحكم في الوصول إلى محيط المنشآت من خلال نظام الدخول بالبطاقات الإلكترونية
  - تُستخدم بوابات دوارة تعمل ببطاقات الاقتراب على جميع نقاط الدخول
  - يجب أن يحمل الموظفون شعار الشركة
  - يجري تسجيل الزوار ويجب عليهم أن يرتدوا شعارًا يُظهر أنهم زوار، وتتم مرافقة الزوار خلال زياراتهم
  - مراقبة الدخول لمحيط المباني والمناطق الآمنة بنظام مراقبة بكاميرات تليفزيونية بمعرفة حراس أمنيين.
- تحتفظ الشركة بسجلات بالوسائط الصادرة والواردة، بما يشمل نوع الوسائط والمرسلين/المستقبلين المخولين والتاريخ والوقت وعدد الوسائط.
- استخدام أنظمة قياسية متنوعة في المجال للحماية من خسارة البيانات بسبب تعطل الطاقة أو تداخل الخطوط.
- استخدام عمليات قياسية في المجال لحذف البيانات الشخصية عند انعدام الحاجة لها.

إدارة الاتصالات وعمليات التشغيل

- تحتفظ الشركة بمستندات أمنية تصف تدابيرها الأمنية والإجراءات ذات الصلة ومسؤولية موظفيها المتمتعين بحق الوصول إلى البيانات الشخصية.
- حفظ نسخ من البيانات الشخصية وإجراءات استعادة البيانات في مكان مختلف عن المكان الواقعة به معدات الكمبيوتر الرئيسي المعالج للبيانات.
- استخدام مكافحات ضد البرامج الضارة للمساعدة في صد البرامج الخبيثة من الدخول غير المصرح به للبيانات الشخصية، بما يشمل البرامج الضارة التي يرجع أصلها للشبكات العامة.
- تشفير بيانات المستخدمة المنقولة عبر الشبكات العامة؟
- سجلات الشركة والوصول إلى أنظمة المعلومات التي تحتوي البيانات الشخصية واستخدامها وتسجيل معرّف الوصول والوقت ومنح التفويض أو رفضه والنشاطات ذات الصلة.

التحكم في الوصول

- تحتفظ الشركة بسجل للموظفين المخول لهم الوصول إلى الأنظمة التي تحتوي بيانات العميل وتقوم بتحديثه.
- تُحدد الشركة الموظفين الذين قد يحصلون على تخويل بمنح البيانات والموارد أو تعديلها أو إلغائها.
- تحرص الشركة أن في حالة تمتع أكثر من شخص بالوصول إلى الأنظمة التي تحتوي على بيانات العميل، فيجب أن يحمل الأفراد معرّفات/سجلات دخول منفصلة.
- لا يُسمح لموظفي الدعم الفني الوصول إلى البينات الشخصية إلا عند الحاجة.
- تُقيد الشركة إمكانية الوصول إلى البيانات الشخصية إلى أولئك الأفراد الذين يحتاجون الوصول إليها لأداء مهامهم الوظيفية.
- تطبق الشركة نظام تحكم في الوصول قائم على الأدوار
- يجرى إبلاغ الموظفين بتعطيل الجلسات الإدارية عند مغادرة المباني أو بخلاف ذلك عند ترك الحواسيب دون مراقبة.
- يجري تخزين كلمات المرور بطريقة تجعلهما غير مفهومة عندما تكون في موضع الاستخدام.
- تستخدم الشركة المعايير القياسية في المجال لتحديد المستخدمين والترخيص لهم ممن يحاولون الدخول إلى أنظمة المعلومات.
- أرست الشركة سياسة لكلمات المرور تمنع مشاركة كلمات المرور، وتُملي ما يجب فعله في حال الكشف عن كلمة المرور وتُلزم بتغيير كلمة المرور بطريقة منتظمة وبتعديل كلمات المرور الافتراضية؛
- تحدد سياسة الشركة لكلمات المرور متطلبات تعقيد كلمات المرور؛
- يجري تخزين جميع كلمات المرور بخوارزمية تجزئة أحادية الاتجاه ولا يجري نقلها بلا تشفير أبدًا
- لدى الشركة ضوابط لمنع الأفراد من الحصول على حقوق للوصول لم تتم منحها لهم للوصول إلى بيانات المستخدم غير المخولين بالوصول إليها
- تحمي جدران نارية قناة الشبكة الداخلية للشركة.
- جميع عمليات نقل البيانات بين الشركة والكيانات والشركاء والعملاء القانونيين محمية ببرتوكول TLS/SSL.

إدارة حوادث الأمن المعلوماتي

- تحتفظ الشركة بسجل للخروقات الأمنية مع وصف الخرق الأمنية والمدة الزمنية وعواقب الخرق واسم المُبلغ واسم المبلَغ له وإجراء استعادة البيانات.

إدارة نقاط الضعف

- يجري فحص الموارد المعلوماتية للشركة بطريقة دورية بماسحات لكشف نقاط الضعف
- تُجري الشركة اختبار اختراق للموارد المعلوماتية وكذلك تدقيقات أمنية

الملحق 2

المعالجون الآخرون

| اسم المعالج الآخر وعنوانه | موضوع التعاقد من الباطن | اختياري: تاريخ إبرام العقد المتعلق بالتعاقد من الباطن |
|---|---|---|
| خدمات ويب أمازون EMEA SARL<br>rue Plaetis 5<br>L-2338 Luxembourg | مقدم مراكز بيانات ومقدم سحابي لخدمات وبرامج الحاسوب الافتراضية.<br><br>مناطق خدمات ويب أمازون EMEA SARL لاستخدام بيانات المستخدم النهائي:<br>ألمانيا – AWS Region Frankfurt (الاتحاد الأوروبي) | |
| Area9 Technologies ApS<br>رقم تسجيل الشركة: 34489343<br>Galionsvej 37, DK 1437<br>Copenhagen K، الدنمارك | دعم تكنولوجيا معلومات واستضافة خوادم | |
| Area9 Labs ApS<br>رقم تسجيل الشركة: 25167406<br>Galionsvej 37, DK 1437<br>Copenhagen K، الدنمارك | دعم تكنولوجيا معلومات واستضافة خوادم | |
| Area9 Innovation ApS<br>رقم تسجيل الشركة: 36921897<br>Galionsvej 37, DK 1437<br>Copenhagen K، الدنمارك | دعم تكنولوجيا معلومات واستضافة خوادم | |
| Area9 Lyceum ApS<br>رقم تسجيل الشركة: 39079976<br>Galionsvej 37, DK 1437<br>Copenhagen K، الدنمارك | دعم تكنولوجيا معلومات واستضافة خوادم | |
| Atlassian B.V.<br>c/o Atlassian, Inc.<br>Bush Street, Floor 13 350<br>San Francisco, CA 94104 | نظام دعم تكنولوجيا المعلومات | |
| AO Kaspersky Lab, 39A/2<br>Leningradskoe Shosse,<br>Moscow, 125212، روسيا الاتحادية | توفير إمكانية الوصول المبدئية للخدمة وتسجيل المديرين | |