# قائمة مراجعة حماية البيانات للجمعية الأوروبية لأبحاث التسويق واستطلاع الآراء (إيسومار)

الجمعية الأوروبية لأبحاث التسويق واستطلاع الآراء (إيسومار)، الرابطة العالمية للأبحاث التسويقية والاجتماعية واستطلاعات الرأي تضم ما يقرب من 4900 عضوًا في 130 بلدًا، وتأتي على رأس المؤسسات التي تهتم بتشجيع الأبحاث التسويقية وتطويرها والرفع من شأنها. يُمكنك الاطلاع على اللوائح والتوجيهات على الموقع الإلكتروني www.esomar.org





© حقوق النشر محفوظة لصالح إيسومار 2015. صدر في يناير 2015. آخر تحديث: ديسمبر 2015.

## المحتويات

## 1 مُقدمة

يواجه الباحثون الذين يعملون في سياق عالمي مجموعة متنوعة من القوانين المحلية التي سُنت بهدف ضمان احترام الخصوصية الفردية وحماية البيانات الشخصية. ولهذا يقع على عاتقهم مسؤولية مراجعة الاشتراطات القانونية في البلد التي يعملون بها والامتثال لها، فضلاً عن اشتراطات حماية البيانات الوطنية في جميع البلدان التي يجرون فيها أبحاثهم و/أو يعالجون فيها البيانات.

وفي الوقت نفسه، فإن التطور المستمر للتكنولوجيات الجديدة ودخولها في جميع جوانب حياتنا لم يتسبب فقط في زيادة حجم البيانات الشخصية التي من الممكن توفرها للباحثين، ولكنه تسبب أيضًا في ظهور أنواع جديدة من المعلومات الشخصية التي يجب حمايتها.

أما الشيء الوحيد الذي لم يتغير فهو حاجة الباحثين إلى حماية سمعة الأبحاث التسويقية والأبحاث الاجتماعية واستطلاعات الرأي عن طريق الالتزام بالممارسات التي تضمن الشفافية للمشاركين والعملاء والثقة في المعلومات التي يقدمونها، والتفكير في المشاركين في الأبحاث.

## 2 النطاق

تم إعداد هذا المستند بهدف تزويد الباحثين، ولا سيما الذين يعملون في المؤسسات الأصغر حجمًا التي قد لا تمتلك الكثير من الموارد أو الخبرة في اشتراطات حماية البيانات، بتوجيهات عامة بشأن مسؤولياتهم في الإطار العالمي لحماية البيانات وذلك لضمان احتفاظ المشاركين في الأبحاث بسيطرتهم على معلوماتهم الشخصية. إن الإطار المحدّد المستخدَم قد تم تطويره من قِبل منظمة التعاون الاقتصادي والتنمية (OECD). يتضمن هذا الإطار مجموعة من ثمانية مبادئ تُستخدم في تصميم البرامج التي تضمن الخصوصية وتحمي البيانات الشخصية، وهذه المبادئ هي:

- حدود جمع البيانات
- نوعية البيانات
- تحديد الغرض
- حدود استخدام البيانات
- وسائل حماية وأمن المعلومات
- الشفافية
- المشاركة الفردية
- المساءلة

تنعكس هذه المبادئ العامة في معظم قوانين الخصوصية وحماية البيانات الحالية والمستجدة في جميع أنحاء العالم.

ومع ذلك، ينبغي على الباحثين ملاحظة أن مبادئ منظمة التعاون والتنمية ترتبط ارتباطًا وثيقًا باشتراطات حماية البيانات في الاتحاد الأوروبي، ونوصي الباحثين العاملين في مناطق أخرى بمراجعة أطر حماية البيانات السارية في تلك المناطق؛ مثل إطار الخصوصية التابع للتعاون الاقتصادي لدول آسيا والمحيط الهادي (APEC)، ومبادئ خصوصية الملاذ الآمن في الولايات المتحدة، ومبادئ الخصوصية المقبولة عمومًا (GAPP) التي وضعها المعهد الأمريكي للمحاسبين القانونيين (AICPA) والمعهد الكندي للمحاسبين القانونيين (CICA). وعلى الرغم من أن هذه الأطر لا تملك عمومًا قوة القانون، فإنها تعبر عن المبادئ الأساسية التي يجب على الباحثين الالتزام بها عند العمل في المنطقة المناسبة.

إضافة إلى ذلك، يجب على الباحثين مراجعة متطلبات الرقابة الذاتية لحماية البيانات والأبحاث التسويقية في كل بلد يخططون القيام فيها بعمل ميداني أو معالجة البيانات، نظرًا لإمكانية وجود اختلافات في طريقة تنفيذ المبادئ الأساسية من بلد إلى أخرى. تمثل التوجيهات الواردة في هذا المستند الحد الأدنى من المعايير اللازمة وقد يصبح من الضروري استكمالها بإجراءات إضافية في سياق مشروع بحثي معين، وقد يجد الباحثون أنه من الضروري الرجوع إلى مستشار قانوني محلي في البلد التي يُجرى فيها البحث لضمان الامتثال التام. وقد يكون من المفيد أيضًا الرجوع إلى قوانين حماية البيانات العالمية، وهي أحد الموارد على شبكة الإنترنت الذي تستضيفه شركة DLA Piper ويتم تحديثه سنويًا.

وأخيرًا فإن الباحثين الذين يجرون أبحاثًا في مجالات متخصصة مثل الرعاية الصحية قد يلزمهم الرجوع إلى توجيهات معينة مثل توجيهات EphMRA للإبلاغ عن الأحداث الضائرة 2014 للحصول على توجيهات إضافية.

## 3 استخدام كلمتي "يجب" و "ينبغي"

تُستخدم كلمة "يجب" في هذه الوثيقة للإشارة إلى الاشتراطات الإلزامية، ونحن نستخدمها عند وصف مبدأ أو ممارسة لابد للباحثين من اتباعها لتحقيق الامتثال للائحة غرفة التجارة العالمية/ جمعية "إيسومار" الدولية حول الأبحاث التسويقية والاجتماعية. وتُستخدم كلمة "ينبغي" عند وصف التنفيذ، وذلك للإشارة إلى أن للباحثين حرية تنفيذ مبدأ أو ممارسة بطرق مختلفة اعتمادًا على تصميم البحث.

## 4 التعريفات

***أبحاث التعاملات التجارية بين الشركات وبعضها (B2B)*** تعني جمع البيانات حول الكيانات القانونية مثل الشركات والمدارس والمؤسسات غير الربحية، وغيرها.

***أبحاث التعاملات التجارية بين الشركات والزبائن (B2C)*** تعني جمع البيانات من الأفراد.

***الموافقة*** تعني الموافقة المستنيرة التي يمنحها الشخص بكامل إرادته لجمع بياناته الشخصية ومعالجتها. في الأبحاث التسويقية والاجتماعية واستطلاعات الرأي، تستند هذه الموافقة إلى تزويد المشارك في البحث بمعلومات واضحة حول طبيعة البيانات التي تُجمع والغرض الذي سوف تُستخدم من أجله وهوية الشخص أو المؤسسة التي تحتفظ بهذه البيانات الشخصية. ويحق للمشارك في البحث سحب موافقته في أي وقت.

***مراقب البيانات*** هو الشخص أو المؤسسة المسؤولة عن تحديد طريقة معالجة البيانات الشخصية. فيصبح الباحث، على سبيل المثال، مراقب البيانات لعملائه أو زبائنه؛ وتصبح وكالة الرعاية الاجتماعية الحكومية مراقب البيانات التي جُمعت من متلقي الرعاية الاجتماعية؛ ويصبح موفر مجموعات المشاركين مراقب البيانات التي جُمعت من أفراد المجموعات على الإنترنت؛ وتصبح شركة الأبحاث مراقب البيانات التي جُمعت من المشاركين في استبيان شامل.

***معالج البيانات*** يعني الطرف الذي يحصل على البيانات الشخصية ويسجلها ويحتفظ بها أو ينفذ العمليات (بما في ذلك التحليل) نيابة عن أو تحت توجيه مراقب البيانات. وكما ذكر أعلاه، فإن شركة الأبحاث سوف تؤدي دوري مراقب البيانات والمعالج في الدراسات الشاملة.

***قوانين حماية الخصوصية*** هي القوانين أو اللوائح الوطنية التي تحمي البيانات الشخصية وتتفق مع المبادئ الواردة في هذا المستند.

***الأبحاث التسوقية*** التي تتضمن الأبحاث الاجتماعية واستطلاعات الرأي، هي التجميع المنهجي للمعلومات حول الأفراد أو المؤسسات وتفسيرها باستخدام الطرق والأساليب الإحصائية والتحليلية للعلوم الاجتماعية التطبيقية وذلك لاكتساب المعرفة أو دعم اتخاذ القرار. ولا يسمح بالكشف عن هوية الشخص المشارك في البحث لمستخدم المعلومات دون موافقة صريحة منه مع ضمان عدم اتخاذ أي نهج للمبيعات تجاهه كنتيجة مباشرة عن المعلومات المقدمة عنه.

***جمع البيانات غير المباشرة*** يعني جمع البيانات بطرق تختلف عن النهج التقليدي الذي يتضمن طرح الأسئلة والإجابة عليها.

***البيانات الشخصية*** تعني أيّ معلومات تخص شخص طبيعي معروف أو يمكن التعرف عليه (في مقابل الشخصية الاعتبارية لمؤسسة أو غيرها من الكيانات المماثلة). والشخص الذي يمكن التعرف على هويته هو الشخص الذي يمكن التعرف عليه بشخصه بطريقة مباشرة أو غير مباشرة بالرجوع إلى رقم الهوية أو خصائص الشخص البدنية أو الفسيولوجية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية. وفي بعض أنواع الأبحاث، قد يتضمن سجل البيانات حالات تسمح بالتعرف على هوية الشخص بسبب الصور أو مقاطع الفيديو أو تسجيلات الصوت أو غيرها من المعلومات الشخصية التي جُمعت أثناء البحث.

***معالجة البيانات الشخصية*** وتتضمن على سبيل المثال لا الحصر: جمع البيانات وتسجيلها وتنظيمها وتخزينها وتغييرها أو تعديلها واسترجاعها والإشارة إليها واستخدامها والكشف عنها بنقلها أو نشرها أو غير ذلك من طرق إتاحتها، أو التخطيط لها أو الجمع بينها أو حظرها أو محوها أو إتلافها بطريقة آلية أو غير ذلك.

***المشارك في البحث*** هو أي شخص تُجمع بياناته الشخصية في مشروع بحثي سواء أكان ذلك بمقابلة مباشرة أو بطرق غير مباشرة.

***الباحث*** هو أي فرد أو مؤسسة تجري مشروعًا بحثيًا أو تقوم بدور استشاري فيه، بما في ذلك الأفراد الذين يعملون في مؤسسات العملاء وأي متعهد فرعي مثل موفر التكنولوجيات المستخدمة.

***عميل البحث أو مستخدم البيانات*** هو أي فرد أو مؤسسة تطلب أو تفوض أو ترعى أو تشترك في مشروع بحثي كامل أو جزء منه.

***البيانات الحسّاسة*** أي معلومات عن الأصل العرقي أو الإثني لشخص يمكن معرفة هويته أو أي معلومات عن صحته أو حياته الجنسية أو سجله الإجرامي أو آرائه السياسية أو معتقداته الدينية أو الفلسفية أو انتمائه النقابي. وقد تتضمن معلومات أخرى في دول مختلفة. في الولايات المتحدة، على سبيل المثال، تُعد كلاً من المعلومات الشخصية المتعلقة بالصحة أو الدخل أو غيرها من المعلومات المالية، أو المعرفات المالية والمستندات التي تصدرها الحكومة أو مستندات الهوية المالية من المعلومات الحسّاسة أيضًا.

***النقل*** عند الحديث عن البيانات يشير المصطلح إلى أي كشف عن البيانات أو إفشائها أو نسخها أو نقلها من طرف إلى آخر بغض النظر عن الوسيلة، بما في ذلك نقلها عبر شبكة إلكترونية، أو النقل المادي، أو نقلها من وسيلة أو جهاز إلى آخر، أو عن طريق الوصول إلى البيانات عن بعد.

***نقل البيانات الشخصية عبر الحدود*** يعني نقل البيانات الشخصية عبر الحدود الوطنية بأي وسيلة، بما في ذلك الوصول إلى البيانات من خارج البلد التي جُمعت بها واستخدام التكنولوجيا السحابية لتخزين البيانات.

## 5 قائمة المراجعة الذاتية لسياسة وإجراءات حماية البيانات

قد يلاحظ مستخدمو قائمة المراجعة أدناه أن العناوين وترتيب العناصر يختلف عن العناوين والترتيب الذي اتبعته منظمة التعاون الاقتصادي والتنمية (OECD). وذلك بهدف صياغة المبادئ باللغة والترتيب الأقرب للباحثين. وقد يجد المستخدمون أيضًا أن هذه

العناصر مرتبطة ببعضها البعض ومتداخلة. **ومع ذلك، فمن الضروري النظر إلى القائمة المرجعية كوحدة كاملة والعناصر الفردية بوصفها عناصر مكملة غير شاملة، مع الأخذ في الاعتبار الاختلافات التي تعتمد على ما إذا كانت المؤسسة تقوم بدور مراقب البيانات أو معالج البيانات. يشير أي سؤال لا تجيب عليه "بنعم" إلى وجود فجوة محتملة في برنامج حماية الخصوصية ومن ثم خطورة مخالفة قانون أو أكثر من قوانين حماية البيانات.**

## 5.1 الحد الأدنى من التأثير

1. عند تصميم مشروع بحثي، هل تقتصر في جمع البيانات الشخصية على العناصر الضرورية لأغراض البحث وتتأكد من عدم استخدامها بأي طريقة لا تتفق مع هذه الأغراض؟

يجب على الباحثين الاقتصار فقط على جمع أو الاحتفاظ بالبيانات الشخصية اللازمة لضمان إجراء مقابلة أو وفقًا لما تتطلبه الرقابة على الجودة أو اختيار العينات أو التحليل. وتتضمن في حالة أبحاث أعمال إلى أعمال، البيانات الشخصية المتعلقة بمنصب المشارك في المؤسسة أو درجته الوظيفية، إذا كانت هذه المعلومات ضرورية لأغراض البحث.

وينطبق المبدأ نفسه على طرق جمع البيانات غير المباشرة التي تجمع فيها البيانات بأي طريقة أخرى بخلاف الطريقة التقليدية لطرح الأسئلة والإجابة عليها. ولذلك فإن من مسؤولية الباحث التأكد من عدم جمع أي بيانات شخصية غير لازمة لأغراض البحث. وفي حالة الحصول على بيانات شخصية إضافية غير لازمة لأغراض البحث، فلابد من فلترتها وحذفها.

2. هل تحرص على اتخاذ التدابير التي تضمن عدم تعرض المشاركين في البحث لأي ضرر أو تأثير سلبي كنتيجة مباشرة على تعاونهم في المشروع البحثي التسويقي؟

يجب على الباحث التأكد من عدم إمكانية تتبع البيانات الشخصية أو التعرف على هوية الشخص بأي طريقة كانت سواء عن طريق التحليل الشامل (الكشف الاستنتاجي)، أو العينات الصغيرة، أو بأي طريقة أخرى تُستخدم فيها نتائج البحث؛ كالجمع بين المعلومات الثانوية مثل بيانات المنطقة الجغرافية أو القدرة على تحديد هوية موظف بعينه في استبيان رضا العملاء.

3. إذا كنت تخطط لاستخدام متعهد فرعي أو جهة خارجية لتقديم بعض الخدمات نيابة عنك، فهل ستكشف لهم عن الحد الأدنى من البيانات الشخصية اللازمة لإجراء الخدمات المتفق عليها؟ هل لديك عقود سارية تضمن تقديم نفس المستوى من حماية البيانات من طرفهم؟

عند استخدام متعهد فرعي، لا تزوده إلا بأقل قدر من البيانات الشخصية اللازمة لتقديم الخدمة المتفق عليها، واحرص على توضيح مسؤوليات المتعهد الفرعي أثناء امتلاكه لهذه البيانات في العقود المبرمة والتعليمات المتداولة بينكما. وعلى جميع المتعهدين الفرعيين الالتزام بنفس القواعد واللوائح التي تلتزم بها المؤسسات البحثية. علاوة على ذلك، لا يُسمح بنقل البيانات الشخصية لمتعهد فرعي أو جهة خارجية إلا بعد الحصول على موافقة مسبقة أو تفويض من عميل شركة الأبحاث.

ويُفترض مما سبق أن المشاركين في البحث سوف يحصلون على ضمان بالحفاظ على سرية بياناتهم التي تم جمعها وعدم تحليلها وتقديم تقارير عنها إلا في شكل إحصائي مُجمع. وإذا قدم المشارك في البحث موافقته على ربط مشاركاته في البحث ببياناته الشخصية، فيجب إبلاغه بطريقة مشاركة هذه المعلومات واستخدامها.

## 5.2 الإخطار والموافقة

4. هل تحصل على موافقة من كل مشارك في البحث تجمع بياناته الشخصية؟

وفقًا لمبادئ سياسة الخصوصية الصادرة عن منظمة التعاون الاقتصادي والتنمية فلا ينبغي الحصول على أي بيانات شخصية إلا بطرق قانونية ونزيهة، وبعلم المشارك في الاستبيان وبعد موافقته، عند الضرورة. وتنص القوانين الوطنية عادةً على عدد من الأسس المشروعة والنزيهة لجمع البيانات، ولكن في معظم الحالات، ينبغي على الباحثين السعي للحصول على موافقة المشاركين في البحث.

وفي حالات أخرى، تقع مسؤولية الحصول على الموافقة على عاتق آخرين؛ عند استخدام مجموعات جهة خارجية أو استخدام قاعدة بيانات العميل. وفي ظل هذه الظروف والظروف المشابهة، يجب على الباحث الحصول على تأكيدات بأنه قد حصل على الموافقة بطريقة صحيحة.

الشروط الواجب توفرها في الموافقة:

- حرة (طوعية مع إمكانية سحبها في أي وقت)
- محددة (تتعلق بغرض أو أكثر من الأغراض المحددة)
- مستنيرة (مع الوعي الكامل بجميع عواقب تقديم الموافقة)

كما يجب إرفاق الموافقة بنص أو إجراء يشير إلى أن المشارك في البحث قد حصل المعلومات الموضحة أدناه. بإيجاز، ينبغي إبلاغ المشارك في البحث (أ) بالغرض الذي سوف تُستخدم فيه بياناته الشخصية (ب) البيانات التي سيتم جمعها تحديدًا (ج) اسم وعنوان ومعلومات الاتصال بالشركة أو المؤسسة التي تجمع البيانات، وإذا لم تكن هي نفس الشركة التي تقوم بدور مراقب البيانات (د) إبلاغه بما إذا كانت البيانات سيتم إفشائها لجهة أخرى أم لا.

ينبغي على الباحثين التفكير مليًا في الطريقة التي يستخدمونها للحصول على الموافقة والتي يعبر عنها عادة بسياسة اختيار الانضمام للدراسة أو تلقي الدعوات بناءً على علاقة سابقة أو تقديم موافقة ضمنية أو مستنيرة أو صريحة. وينبغي توثيق الطريقة المستخدمة تحديدًا.

وبوجه عام، كلما كانت البيانات التي يتم جمعها أكثر حساسية أو اقتحامًا للخصوصية أو كانت غير واضحة، كانت معايير الموافقة اللازمة أعلى. وفي بعض الدول، توجد فئات محددة من "البيانات الشخصية الحسّاسة" التي تتطلب الحصول على موافقة صريحة من الأفراد المعنيين قبل جمعها.

قد توجد بعض الحالات التي يجمع فيها الباحث أو يتلقى بيانات شخصية عن غير قصد أو من غير المشاركين في البحث؛ كالمعلومات التي يتطوع المشاركون بالإدلاء بها، أو القوائم التي قدمها العملاء وتحتوي على معلومات أكثر من المعلومات اللازمة في البحث، أو غير المشاركين الذين التُقطت لهم صورًا أو مقاطع فيديو. وينبغي على الباحثين التعامل مع هذه المعلومات على النحو الذي يتعاملون به مع البيانات الشخصية. فينبغي إزالة خصائص تعريفها أو إتلافها على الفور، خاصة إذا لم يكن هناك أي طريقة لإبلاغ الناس الذين جُمعت معلوماتهم عن مكانها أو تخزينها أو استخدامها. وفي بعض الدول، يصبح من اللازم حذف مثل هذه البيانات أو التعامل معها بنفس طريقة التعامل مع معلومات أخرى تم جمعها عمدًا.

5. هل أنت صريح بخصوص الغرض أو الأغراض التي تجمع من أجلها هذه البيانات وتحتفظ بها؟

حرص قطاع البحث منذ أمد طويل على التمييز بين الأبحاث التسويقية وجمع البيانات لأغراض مثل الإعلان وترويج المبيعات ووضع القوائم والتسويق والبيع المباشرين. ويعد هذا التمييز مكونًا أساسيًا في تفرقة الغرض وتعزيز الصورة الإيجابية للبحث في أروقة الجهات الرقابية وبين الجمهور. وفي السنوات الأخيرة، أدى ظهور التكنولوجيات الجديدة إلى زيادة فرص جمع المعلومات الشخصية من خلال الطرق التي تشمل التتبع على الإنترنت وتنزيلات تطبيقات الهاتف المحمول. وفي جميع الحالات، من الضروري قبل جمع أي بيانات إبلاغ المشاركين المحتملين في البحث بأغراض البحث التي سيتم استخدام هذه البيانات فيها وأي عواقب محتملة قد تنتج عنها بما في ذلك التواصل معهم للمتابعة لأغراض الجودة.

وتُعد الشفافية مع المشاركين في البحث عنصرًا لا غنى عنه في الإشعار المُقدم لهم عند جمع بيانات شخصية لاستخدامها في أغراض أبحاث السوق. فيجب تقديم معلومات كافية للمشارك في البحث حول الاستخدام المقصود من البيانات الشخصية التي يتم جمعها وإمكانية مشاركتها مع جهات خارجية. فمثلاً إذا كان الغرض من استخدام البيانات الشخصية هو ربط المشاركة في الاستبيان بملفه كعميل، فيجب إخطار المشارك في البحث بذلك عند جمع البيانات الشخصية منه.

يجب مراجعة إشعارات الخصوصية بانتظام للتأكد من أن نوع البيانات التي يتم جمعها والغرض من استخدامها لم يتغير، ويجب على الباحثين ضمان أن ممارسات العمل الفعلية والتكنولوجيات المستخدمة في المؤسسات البحثية تتفق مع التزاماتهم تجاه المشاركين في البحث وتمتثل للاشتراطات الرقابية التي تشهد تطورًا مستمرًا. وكذلك لابد من تحليل كل غرض من أغراض استخدام البيانات الشخصية لضمان الامتثال لقوانين الخصوصية المحلية ولائحة غرفة التجارة العالمية/ جمعية "إيسومار" وتوجيه جمعية "إيسومار"، وضمان اتساقها أيضًا مع وعود الخصوصية التي قدمها الباحث للمشاركين في البحث.

6. هل أنت صريح بخصوص البيانات التي سيتم جمعها على وجه التحديد؟

نظرًا لأن بعض الدول قد وضعت تعريفًا واسعًا للبيانات الشخصية، فيجب على الباحث التفكير في كل عناصر البيانات الشخصية الممكنة التي قد يتم جمعها أثناء إعداد إشعار المشارك في البحث. وقد تتضمن البيانات الشخصية الاسم والعنوان وعنوان البريد الإلكتروني ورقم الهاتف وتاريخ الميلاد ومعرف الهاتف المحمول وعنوان برتوكول الإنترنت والصور وتسجيلات الصوت والفيديو وأرقام بطاقات التعريف الوطنية (رخصة القيادة والضمان الاجتماعي والتأمين الوطني)، وبطاقة التعريف التي أصدرتها لك المؤسسة التي تعمل بها واسم المستخدم في مواقع التواصل الاجتماعي والبيانات المخزنة في ملفات الارتباط وبكسل / علامة التتبع. تذكر أيضًا أن عنصرًا واحدًا من البيانات قد لا يسمح وحده بالتعرف على هوية صاحبه وفقًا للقانون المحلي، ولكن عند جمعه مع بيانات أخرى (مثل الرمز البريدي أو الجنس أو محل العمل أو المدرسة أو المنصب والراتب)، فقد يسمح بالتعرف على الفرد بعينه.

إضافة إلى ذلك، يجب الأخذ في الاعتبار كل من يمكنهم الحصول على البيانات الشخصية مثل الباحثون ووكالات الأبحاث والجهات الخارجية مقدمي الخدمات و/أو العملاء، فقد يكون لكل منهم القدرة على جمع واستخدام البيانات الشخصية في سياق مشروع بحثي.

7. هل أنت صريح بخصوص طرق جمع البيانات، بما في ذلك أي طرق غير مباشرة قد لا يكون المشارك في البحث على علم بها؟

تاريخيًا، اعتمد البحث على إجراء المقابلات كوسيلة أساسية لجمع البيانات الشخصية. وكما لاحظنا في السؤال رقم (5) أعلاه، فقد أتاحت التكنولوجيا الحديثة الحصول على مجموعة واسعة من البيانات الشخصية دون علم أصحابها. لذلك يجب إبلاغ جميع المشاركين في البحث بالبيانات المحددة التي يجري جمعها والطرق المستخدمة في ذلك، سواء بالطرق المباشرة مثل إجراء المقابلات أو الطرق غير المباشرة مثل استخدام تطبيقات الهاتف المحمول أو تتبع السلوك عن طريق ملفات الارتباط على الإنترنت.

وينبغي على الباحث الأخذ في الاعتبار نوعية البيانات التي تم جمعها وطرق جمعها التي قد تكون غير متوقعة بالنسبة للمشارك في البحث، وتزويده بالمعلومات المناسبة عن هذه الطرق. فكر في تقديم إشعارات "نموذج قصير" مع إشعار الخصوصية الأكثر تفصيلاً لوصف جمع البيانات أو لوصف استخدام الطرق غير المتوقعة أو التفصيلية. أما تطبيقات الهاتف المحمول، وبخاصة تلك التي تتضمن الموقع الجغرافي، أو ميزة "الاستماع غير المباشر" أو تحديد نظام تشغيل الهاتف المحمول، فكلها تتطلب وصفًا تفصيليًا وموافقة صريحة من المشاركين في البحث على مثل هذه الأنشطة.

## 5.3 السلامة / الأمن

8. هل تتخذ أي إجراءات تضمن أن تكون جميع البيانات الشخصية التي تُجمع دقيقة وكاملة وحديثة؟

ينبغي إجراء فحوصات الجودة في كل مرحلة من مراحل إجراء البحث. عند صياغة استبيان أو تطبيقات بحثية، ينبغي إجراء اختبار قبل بدء العمل الميداني لتقليل احتمال حدوث أخطاء في جمع البيانات. وينبغي خلال مرحلة جمع البيانات مراقبة البيانات الواردة والتحقق من صحتها وفقًا لمعايير جودة الأبحاث المطبقة. وأثناء مراحل معالجة البيانات وإعداد التقارير، ينبغي القيام بفحوصات جودة إضافية لضمان صحة البيانات وضمان اتساق التحليل والنتائج والتوصيات مع البيانات.

أما الباحثين الذين يعملون مع مجموعات المشاركين في البحث، فينبغي عليهم التأكد من قدرة أفراد المجموعة على مراجعة وتحديث بياناتهم الشخصية في أي وقت، وينبغي تذكيرهم بالقيام بذلك دوريًا. وينبغي على العينات المختارة من المجموعات تحديث معلوماتهم الديموغرافية. تعد لائحة ISO 26362:2009 – مجموعات المشاركين المحتملين في الأبحاث التسويقية والأبحاث الاجتماعية واستطلاعات الرأي مصدرًا جيدًا للممارسات القياسية في هذا الصدد.

9. هل تضمن عدم الاحتفاظ بالبيانات الشخصية لمدة أطول مما تتطلبه أغراض جمع هذه المعلومات أو معالجتها؟ هل لديك إجراءات للاحتفاظ بمعلومات تحديد الهوية أو حذفها بشكل منفصل من سجلات البيانات بمجرد انتهاء الحاجة إليها؟

ينبغي أن يحدد الباحثون فترات الاحتفاظ بالبيانات بأقصر فترة ممكنة، على أن يضعوا في الحسبان في جميع الأحوال القوانين المعمول بها ومصدر البيانات التي يجمعونها وما إذا كان دورهم هو مراقبة البيانات أم معالجتها. وفي هذه الحالة، قد يحدد العملاء فترات الاحتفاظ بالبيانات بنص في العقود التي تبرم فيما بينهم.

وبغض النظر عن مصدر البيانات الشخصية، فإن المعلومات المستمدة من الدراسات الطولية أو المعلومات الشخصية عن أعضاء المجموعات عادة ما يتم استخدامها والاحتفاظ بها طوال الوقت الذي يبقى فيه الأعضاء نشطين في المجال. وعلى النقيض من ذلك، ينبغي أن تكون فترات الاحتفاظ بالبيانات الشخصية أقصر بكثير في حالة المشاركين الذين لا ينتمون إلى أي مجموعة وانتهت مشاركتهم في بحث معين، على ألا يتم إتلاف هذه البيانات قبل إجراء فحوصات الجودة أثناء مرحلة معالجة البيانات لضمان الجودة واستيفاء اشتراطات مبدأ سلامة البيانات في سياسة الخصوصية.

عند استخدام البيانات الشخصية، من الأفضل استخدامها تحت اسم مستعار. ويجب الاحتفاظ بملف رئيسي يربط أسماء المشتركين أو عناوينهم أو أرقام هواتفهم بأرقام التعريف التي تم إنشائها داخليًا في مكان آمن مع قصر إمكانية الحصول عليها على عدد صغير من الناس مثل موظفي اختيار العينات أو إدارة المجموعات. وبالتالي، يصبح بإمكان الباحثين أو موظفي معالجة البيانات أو موظفي الترميز الذين يحتاجون إلى تحليل البيانات على مستوى المشارك القيام بعملهم دون معرفة أسماء المشاركين أو عناوينهم أو أرقام هواتفهم.

بعد معالجة المشاركات في الاستبيان وإعداد تقارير بها في صورة بيانات إحصائية مجمعة، ينبغي حذف البيانات الشخصية للمشاركين والهويات المستعارة حتى لا تمتلك المؤسسات البحثية أي بيانات شخصية.

10. هل تتبع أي إجراءات للاستجابة لطلبات الأفراد المتعلقة بالبيانات الشخصية التي قد تكون جمعتها منهم؟ هل تتضمن الإجراءات الخاصة بك للتعامل مع طلبات الحصول على البيانات التحقق من هويات مقدمي الطلبات وإجابة طلباتهم في إطار زمني معقول والسماح لهم بتصحيح البيانات غير الدقيقة أو حذف البيانات بشكل كامل؟

ينبغي وضع إجراءات رسمية والإعلان عنها والالتزام بها للرد على الأفراد الذين يرغبون في الحصول على البيانات الشخصية التي تحتفظ بها المؤسسات عنهم. ويجب التحقق من صحة هويات الأفراد الذين يقدمون طلبات للحصول على البيانات لمنع الكشف عن البيانات الشخصية لأشخاص آخرين بصورة غير لائقة.

وبمجرد التحقق من صحة هوية الأفراد الذين يقدمون طلبات الحصول على البيانات - أي التحقق من أن هوية هذا الشخص هو ما يدعيه وأن لديه الحق في الحصول على البيانات محل الطلب - ينبغي على الباحثين السعي لتلبية طلب الحصول على البيانات بأسرع وقت ممكن، أي في غضون من 10 إلى 30 يومًا بحسب القوانين المعمول بها. وإذا طلبت شركة الأبحاث وقتًا إضافيًا لتلبية الطلب، فبإمكانها تمديد الموعد النهائي الذي ينص عليه القانون، شريطة إخطار الفرد بذلك وأن تكون أسباب تمديد الموعد النهائي منطقية. وقد يكون هذا الوقت الإضافي ضروريًا لإجراء مشاورات بشأن الطلب أو لجمع المعلومات المطلوبة من قواعد بيانات متعددة.

وبالرغم من أن قوانين حماية البيانات قد تتضمن استثناءات تشترط على المؤسسات رفض حصول الأفراد على المعلومات الشخصية في مواقف معينة، فعلى الأرجح أن هذه الاستثناءات لا تنطبق على المعلومات الشخصية التي يتم معالجتها في سياق الأبحاث التسويقية. فعلى سبيل المثل، قد تسمح القوانين المعمول بها للمؤسسات برفض طلبات الحصول على المعلومات إذا كانت هذه المعلومات تندرج تحت مبدأ سرية المعلومات بين المحامي وموكله. ومثال آخر على ذلك، إذا كانت المؤسسة البحثية قد أفشت معلومات لمؤسسة حكومية لإنفاذ القانون أو لأسباب تتعلق بالأمن القومي، ففي هذا الموقف قد توصي المؤسسة الحكومية المؤسسة البحثية برفض طلب الحصول على البيانات أو عدم الكشف عن البيانات التي تم إفشائها.

11. هل هناك بروتوكولات أمن لكل مجموعة بيانات تحمي من مخاطر مثل فقدها أو الحصول عليها بدون تصريح أو إتلافها أو استخدامها أو تعديلها أو الكشف عنها؟

يبدأ الوفاء بهذه الالتزامات بوضع وتنفيذ سياسة أمنية لحماية المعلومات الشخصية وغيرها من أنواع المعلومات السرية الأخرى. ويعد ISO 27001 معيارًا معترف به لأمن المعلومات يمكن أن تستند إليه أي سياسة أمنية شاملة.

ويشمل استخدام الضمانات الأمنية المناسبة لتوفير الحماية اللازمة ما يلي:

- التدابير المادية (الخزائن المقفلة لحفظ الملفات وتقييد الوصول إلى المكاتب ونظم الإنذار وكاميرات الأمن)
- الأدوات التكنولوجية (كلمات السر والتشفير والجدران النارية)
- الضوابط التنظيمية (التحريات، والقواعد المتعلقة باصطحاب أجهزة الكمبيوتر خارج محل العمل، وقصر الحصول على البيانات على أساس "الحاجة إلى المعرفة"، وتدريب الموظفين، والاتفاقات مع العملاء والمتعهدين الفرعيين)

ينبغي أن تتضمن سياسة الأمن أيضًا إجراءات للتعامل مع أي خرق محتمل للبيانات يتسبب في الكشف عن بيانات شخصية. وإذا كانت هذه البيانات قد جمعتها ووفرتها جهة أخرى، كأن تكون قاعدة بيانات العميل، فيجب إبلاغ هذه الجهة على الفور. كما يجب إخطار المشاركين الذين تم الكشف عن بياناتهم إذا كان هذا الكشف يعرضهم لبعض المخاطر (مثل سرقة الهوية) والخطوات التي تم اتخاذها لحمايتهم من هذا الخطر.

12. هل هناك بيان واضح حول طول الفترة التي يتم الاحتفاظ بالبيانات الشخصية فيها؟

وقد تختلف طول الفترة الزمنية للاحتفاظ بالبيانات الشخصية من مشروع بحثي لآخر اعتمادًا على مجموعة متنوعة من الظروف المذكورة آنفا في الرد على السؤال رقم 9.

وبالرغم من أن ممارسات الاحتفاظ عادة ما تكون مدرجة في سياسات الخصوصية، فقد يكون من الأفضل لأسباب عملية عدم الإعلان عن جداول زمنية دقيقة للاحتفاظ بالبيانات في أنواع مختلفة من الدراسات. ولذلك، ينبغي على الباحثين التفكير في الإعلان عن معلومات الاحتفاظ بالبيانات في مواد التوظيف في الدراية أو مقدمات الاستبيانات أو نماذج الموافقة الخاصة بالدراسة. وينبغي أن يكونوا على استعداد دائمًا للإعلان عن جداول الاحتفاظ بالبيانات الخاصة بمشروع معين عند الطلب.

## 5.4 نقل البيانات

13. هل ذكرت على وجه التحديد القواعد والإجراءات التي تحكم استخدام البيانات الشخصية والكشف عنها؟

ترد هذه القواعد والإجراءات بشكل واضح في قوانين الخصوصية وحماية البيانات المحلية الموجودة في بلدك. وينبغي توثيق تفسير لما يعنيه هذا توثيقًا واضحًا بالعمليات والمستندات المكتوبة لضمان إمكانية تنفيذ الموظفين للإجراءات الخاصة بإدارة البيانات الشخصية وعلى دراية بهذه القواعد والإجراءات. فعلى سبيل المثال، هذا يشمل مبدأ ضرورة الحصول على موافقة من المشارك في البحث قبل الكشف عن أي من هذه البيانات، حتى للعملاء أو الباحثين في مؤسسات العملاء.

14. هل الشروط التي يتم الكشف عن المعلومات الشخصية بموجبها واضحة وغير مبهمة؟

يجب على المشاركين في البحث معرفة ما يحدث لبياناتهم الشخصية، وهو ما يجب توضيحه إما لفظيًا أو في شكل مكتوب أو مستند يشير إلى أن المشارك في البحث قد وافق - أي عبر موافقتهم التي يتم تسجيلها كدليل على أنهم قد وافقوا.

15. هل موظفوك على علم بهذه القواعد ومدربون على طريقة تنفيذ هذه الإجراءات؟

توضح سياسة الخصوصية الخاصة بك ممارسات جمع البيانات وإدارتها الخاصة بشركتك. من المهم أيضا وضع إجراءات التشغيل الأساسية الداخلية (SOPs) لضمان الالتزام بوعود الخصوصية التي قُدمت للمشاركين.

ينبغي أن يتضمن تدريب الموظفين مراجعة سريعة للقوانين المعمول بها ولوائح السلوك الخاصة بالقطاع وسياسات خصوصية التعامل مع العملاء وإجراءات التشغيل الأساسية. ينبغي تقديم تدريب الخصوصية مرة على الأقل سنويًا وينبغي إعداد تقارير بالحضور كذلك.

ينبغي أن يتمكن جميع الموظفين المسؤولين عن التعامل مع العملاء من توضيح سياسات وإجراءات الشركة على مستوى عال. إذ ينبغي عليهم معرفة مع من يتواصلون داخليًا للحصول على المساعدة عند وجود استفسارات لا يعرفون إجابتها.

فضلاً عن ضرورة وجود إشراف واضح وتحديد المسؤوليات بحيث تتضمن شكلاً من أشكال المراقبة على الإجراءات المُتبعة.

## 5.5 نقل البيانات الشخصية عبر الحدود

16. إذا كانت البيانات الشخصية سيتم نقلها من بلد لأخرى، فهل يتم القيام بذلك بطريقة تلبي اشتراطات حماية البيانات في كل من بلدي الأصل والوجهة؟

يُشار إلى هذه العملية عادة باسم "نقل البيانات الشخصية عبر الحدود". وتحدث عند جمع البيانات عبر الحدود الوطنية و/أو عند معالجة البيانات بالخارج أو الاستعانة بمصادر خارجية من دولة أخرى كأن يوظف العميل باحثًا في بلد آخر لإجراء دراسة باستخدام زبائن العميل أو بيانات مستخدم الخدمة. ولكل دولة قواعدها الخاصة بكيفية معالجة مثل هذه البيانات وحمايتها التي لابد للباحثين الالتزام بها. وبالرغم من أن هذا قد يبدو معقدًا، إلا أنه مفيد عند تحليل قضايا الامتثال التي يواجهها الباحثون إلى ثلاث قضايا رئيسية:

- ضمان إجراء عملية نقل البيانات الشخصية عبر الحدود بالامتثال للقوانين الوطنية المعمول بها. ومن أكثر الأسس شيوعًا التي تضمن الحماية الكافية لنقل البيانات بين الحدود إما الموافقة أو استخدام بنود تعاقدية مناسبة، والحصول على تصريح مسبق، إذا اقتضت القوانين السارية ذلك، من هيئة حماية البيانات الوطنية أو غيرها من السلطات الرقابية للخصوصية لاستخدام تلك العقود. وكتدبير أمني إضافي ولتقليل المخاطر عند معالجة البيانات في الخارج، ينبغي إزالة البيانات الشخصية التي تسمح بمعرفة هوية صاحبها إذا أمكن بحيث لا يبقى سوى رقم التعريف المستعار لاستخدامه في ربط البيانات الخاصة بالأفراد مع هوية المشارك.

- قدرة الباحث على نقل البيانات عبر الحدود عند القيام بوظيفة معالج البيانات، أي عند إجراء دراسة باستخدام عينة قدمها العميل. وحتى في الحالات التي يقوم فيها الباحثون بما يلزم لضمان امتثال عمليات نقل البيانات عبر الحدود للقواعد التي تحكم مثل هذه التحويلات، ينبغي أن يضعوا في اعتبارهم عند معالجة البيانات الشخصية كمعالج للبيانات يعمل نيابة عن مراقب البيانات (عميل الباحث، على سبيل المثال) ، فقد لا يتمكنون، بوصفهم مراقب البيانات، من السماح بإجراء عمليات نقل البيانات الشخصية التي يراقبونها عبر الحدود، مما يؤثر على الطريقة التي يقدرون فيها على تنفيذ المشروع. ينبغي أن يكون هناك اتفاق مكتوب بين الطرفين بخصوص ما سبق.

- عمليات تحويل البيانات الشخصية عبر الحدود عند جمع البيانات الشخصية من المشاركين في البحث في بلدان أخرى؛ مثل: الاستبيانات على الإنترنت الموجهة للمشاركين المقيمين في بلد (بلدان) أخرى مختلفة عن البلد التي يقيم فيها الباحث المراقب للدراسة. وعادة ما تكون قوانين الخصوصية المعمول بها هي القوانين المحلية في الدولة التي يقيم فيها الباحث. ومع ذلك، يجب على الباحث التأكد من أن الدراسة أو المجموعة تمتثل مع أي قوانين محلية أخرى معمول بها في الدول التي يتم جمع المعلومات منها. تشمل الممارسات الموصى به ضمان: (1) أن ترد التفاصيل القانونية للباحث (اسم الشركة والعنوان البريدي وغيرها) داخل البلد في جميع مواد توظيف المشاركين في البحث؛ (2) أن تتضمن سياسة الخصوصية على الإنترنت بيان بسيط وواضح يشير إلى عمليات تحويل

البيانات عبر الحدود التي سوف تجري إذا شاركت في الدراسة أو الاستبيان (3) الإشارة إلى عمليات تحويل البيانات عبر الحدود في إطار الموافقة على الانضمام إلى الاستبيان.

### 5.6 التعهيد الخارجي والتعهد الفرعي

17. هل هناك اشتراطات واضحة تشمل الرقابة المناسبة على أي معالج خارجي للبيانات أو غيرهم من المتعهدين الفرعيين؟

لابد من وجود اشتراطات واضحة يتم الإعلان عنها لجميع معالجي البيانات الخارجيين أو غيرهم من المتعهدين الفرعيين للالتزام بقواعد حماية البيانات اللازمة المتعلقة بالبيانات الشخصية عند أي شكل من أشكال نقل البيانات. وينبغي الحرص على تقديم حماية إضافية عند نقل أي بيانات، سواء كانت على مستوى شخصي أو مستوى مجمع باستخدام عمليات تكنولوجيا المعلومات المخصصة مثل تشفير البيانات عند نقلها أو استخدام منصات نقل بروتوكول نقل الملفات الآمنة. إذا كان من اللازم إنشاء نسخ من أي بيانات كنسخة احتياطية من المتعهدين الفرعيين أو معالجي البيانات الخارجيين، فيجب وضع عمليات واضحة لحماية هذه البيانات أثناء تخزينها وحذفها عندما لا تعد هناك حاجة لها.

### 5.7 سياسة الخصوصية

18. هل تتوفر معلومات حول الخصوصية وبرنامج حماية البيانات الشخصية وفي شكل يسهل على المشاركين فهمه؟

تشترط العديد من الدول إتاحة المعلومات المتوفرة في سياسة الخصوصية للمشاركين في البحث. وبالرغم من أن المحتوى والتفاصيل تختلف من بلد لأخرى، فلابد للباحثين دائمًا تعريف أنفسهم بوضوح للمشاركين في البحث والتأكد من توضيح غرض البحث، وطريقة جمع البيانات الشخصية وإدارتها (تخزينها واستخدامها والحصول عليها والكشف عنها)، وطريقة الحصول على مزيد من المعلومات أو تقديم شكوى.

لابد للباحثين التأكد من أن السياسات سهلة الفهم وذات صلة بالقارئ ومن السهل العثور عليها وموجزة بقدر الإمكان، ومصمّمة خصيصًا لعمليات المؤسسة. وهو ما يشمل توفير السياسات بجميع اللغات المناسبة ومراجعة السياسات بانتظام وتحديثها حسبما تقتضي الحاجة.

19. هل هوية ومسؤولية مراقب البيانات معروفة وواضحة؟

لابد للباحثين الحرص على توضيح دورهم ومسؤولياتهم في إدارة البيانات الشخصية للمشاركين في البحث. وتشمل تحديد هوية مراقب البيانات وإذا ما سوف يتم الاستعانة بأي معالج بيانات خارجي. ويجب عدم ترك المشاركين في حيرة بخصوص هوية المؤسسة المسؤولة عن إدارة بياناتهم.

وتشترط بعض الدول أيضًا تعيين أفراد بعينهم بوصفهم المسؤولين عن ممارسات حماية البيانات في الشركة.

وفي حالة الاستبيانات مستترة الأسماء التي تستخدم عينات العميل، ينبغي إبلاغ المشاركين في بداية المقابلة أنه لن يتم الكشف عن اسم العميل حتى نهاية الاستبيان لأن الكشف عن هذه المعلومات في البداية قد يؤدي إلى تحيز في الإجابة. ونظرًا لأن العديد من قوانين حماية البيانات الوطنية تعطي المشاركين الحق القانوني في معرفة ممن حصل الباحث على بياناتهم الشخصية، فلابد للباحثين أن يكونوا على استعداد لتحديد اسم العميل في أي وقت بناءً على طلب من المشاركين.

20. هل من الواضح أن مراقب البيانات مسؤول عن البيانات الشخصية الموجودة تحت تصرفه بصرف النظر عن مكانها؟

إذا كان من المحتمل أن يقوم الباحث بالتعهد الفرعي لعملية المعالجة أو نقل البيانات الشخصية خارج الدولة، فعليه الاستعداد لتزويد مراقب البيانات بتفاصيل المتعهد الفرعي ومواقع المعالجة، وينبغي عليه الحصول على موافقة مسبقة من مراقب البيانات إذا لزم الأمر. وإذا كانت وكالة الأبحاث هي مراقب البيانات، فعليها الإشارة في سياسات الخصوصية الخاصة بها إلى استخدام معالجي البيانات ووضع قائمة بالبلدان أو المناطق المحيطة التي تتم فيها. وينبغي على الباحثين الانتباه إلى حقيقة أن بعض الدول تمنع الباحثين من نقل البيانات الشخصية إلى دول أو مناطق ليس لديها مستويات مماثلة من قانون حماية البيانات. بشرط الامتثال للقواعد التي تحكم نقل البيانات عبر الحدود والتي يفرضها القانون الوطني المحلي ذو الصلة، يسمح بنقل المعلومات الشخصية عبر مجموعة متعددة الجنسيات في معظم الدول، بالرغم من أن بعضها لا يزال يشترط إخطار موضوعات البيانات بمواقع وجود البيانات.

## 6 قضايا خاصة

### 6.1 جمع البيانات من الأطفال

تختلف القوانين الوطنية التي تحدد الأعمار التي لم تعد فيها موافقة الوالدين ضرورية اختلافًا كبيرًا من بلد لأخرى، ويجب على الباحثين مراجعة القوانين الوطنية ولوائح الرقابة الذاتية في الدول التي يتم جمع البيانات بها لتحديد الحالات التي يلزم فيها الحصول على إذن الوالدين أو الحساسيات الثقافية التي تتطلب معاملة خاصة. وفي غياب المبادئ التوجيهية الوطنية، يُرجى الرجوع إلى توجيه جمعية "إيسومار"، إجراء المقابلات مع الأطفال والشباب اليافعين.

ويتطلب جمع البيانات من الأطفال الحصول على إذن يمكن التحقق من صحته من الوصي القانوني على الطفل. ولابد من تزويد الوالد أو المسؤول عنه بمعلومات كافية حول طبيعة المشروع البحثي لمنحه القدرة على اتخاذ قرار مستنير بشأن مشاركة الطفل. وينبغي أن يسجل الباحث هوية البالغ المسؤول عن الطفل وعلاقته به.

### 6.2 أبحاث التعاملات التجارية بين الشركات وبعضها

عدد ضخم من المشروعات البحثية التي تتضمن جمع البيانات من الكيانات القانونية مثل الشركات أو المدارس أو المنظمات غير الربحية والمؤسسات المماثلة. وهذه الأبحاث غالبًا ما تتضمن جمع المعلومات عن هذه الكيانات مثل الإيرادات وعدد الموظفين والقطاع والمكان وغير ذلك.

وفي كل هذه الحالات يحق للمؤسسات المشاركة التمتع بنفس المستوى من الحماية المكفولة للأفراد المشاركين في أشكال أخرى من الأبحاث وعدم الكشف عن هوياتها عند إعداد التقارير.

جدير بالذكر أن العديد من قوانين حماية البيانات الوطنية تعامل المسمى الوظيفي ومعلومات الاتصال في محل العمل معاملة البيانات الشخصية. وتذهب بعض قوانين حماية البيانات إلى ما هو أبعد من ذلك، حيث تطبق شروطها على الأشخاص الطبيعيين والاعتباريين (مثل الأفراد والكيانات القانونية).

### 6.3 الصور وتسجيلات الصوت والفيديو

تتجه العديد من تقنيات الأبحاث الجديدة إلى إنشاء أو تخزين أو بث الصور ومقاطع الصوت والفيديو كجزء من عملية البحث. ومن الأمثلة البارزة على ذلك أبحاث علم الأجناس البشريّة والتسوق المقنّع.

ويجب على الباحثين معرفة أن الصور وتسجيلات الصوت والفيديو قد تكون بيانات شخصية وإذا كانت كذلك فيجب التعامل معها بنفس الطريقة. إذا طلب الباحثون من المشاركين تقديم معلومات بأي من هذه الأشكال، فينبغي عليهم تقديم الإرشادات اللازمة بشأن طريقة الحد من جمع البيانات غير المرغوب فيها، وخصوصًا من غير المشاركين.

وأخيرًا، قد تتضمن بعض أنواع الدراسات الرصدية التصوير وتسجيل الصوت والفيديو في الأماكن العامة مما يشمل بعض الذين لم يتم توظيفهم للمشاركة في البحث. وفي مثل هذه الحالات يجب على الباحثين الحصول على إذن لتبادل هذه الصور من الأفراد الذين تظهر وجوههم بوضوح ويمكن التعرف عليها. وإذا لم يكن من الممكن الحصول على إذن، فيجب تنقيط صورة الأفراد أو إخفاء هويتهم. إضافة إلى ذلك، ينبغي وضع علامات واضحة ومقروءة للإشارة إلى أن المنطقة تحت الملاحظة وإضافة تفاصيل الاتصال الخاصة بالفرد أو المؤسسة المسؤولة. وينبغي وضع الكاميرات بحيث ترصد فقط المساحات المراد مراقبتها.

### 6.4 التخزين السحابي

ينبغي النظر في قرار تخزين البيانات الشخصية في السحابة بعناية. فعليهم تقييم الضوابط الأمنية لمقدمي خدمة التخزين السحابية والشروط والأحكام الأساسية الخاصة بها. ولا يقدم العديد من مقدمي خدمة التخزين السحابية سوى تعويضات ضعيفة في حال تسببها بخروقات أمنية وتعريض البيانات الشخصية للخطر. وهذا يعني أن شركة الباحث تأخذ مخاطرة بالتعرض لأضرار وخسائر مالية تنجم عن انتهاكات الخصوصية الخطيرة التي تؤدي إلى ضرر للأفراد أيضًا.

ولذلك ينبغي على الباحثين وضع ضوابط تعويضية للحماية من هذه المخاطر. فينبغي عليهم، مثلاً، تشفير البيانات الشخصية عند نقلها (النقل إلى/من السحابة) وفي وقت (تخزينها على خوادم مقدم السحابة)، والتفكير في شراء بوليصة تأمين ضد مخاطر الإنترنت.

كما يجب على الباحثين النظر في مواقع تخزين البيانات الشخصية لتحديد ما إذا كان استخدام التخزين السحابي نوع من أنواع النقل عبر الحدود أم لا. راجع الفقرة 5.5 من هذا المستند لمزيد من المعلومات. يوفر بعض مقدمي الخدمات السحابية مواقع تخزين خاصة لكل بلد وهو ما قد يكون مفيدًا في بعض الحالات.

وأخيرًا، ينبغي على الباحثين وضع البيانات الشخصية على سحابة خاصة، وليس عامة. والسحابة الخاصة هي السحابة التي يتم فيها تخصيص المعدات الموجودة في مركز بيانات محدد لشركة الباحث. ومن أهم فوائد السحابة الخاصة معرفة الباحث دومًا بموقع البيانات الشخصية. وعلى النقيض من ذلك، فقد يؤدي استخدام سحابة عامة إلى وجود البيانات في مركزين أو أكثر من مراكز البيانات وفي قارتين أو أكثر، مما يثير قضايا الامتثال المحتملة، سواء مع الاشتراطات السارية بموجب قوانين حماية البيانات ومع العقود التي أبرمت مع مراقبي البيانات، والتي تحدد الموقع الذي يجب وضع البيانات الشخصية فيه.

### 6.5 إخفاء الهوية والهوية المستعارة

جزء أساسي من مسؤولية حماية البيانات التي تقع على الباحث هو إخفاء هوية البيانات قبل الكشف عنها لعميل أو حتى لعامة الناس. إخفاء الهوية هو أحد إجراءات الحماية التي تتضمن إما حذف أو تعديل المعرفات الشخصية لتقديم البيانات في شكل لا يسمح بالتعرف على الأفراد. مثل طمس الصور لإخفاء الوجوه أو تقديم تقارير بالنتائج في صورة إحصائيات مجمعة للتأكد من أنها لن تسمح بتحديد فرد بعينه.

أما استخدام الأسماء المستعارة فيتضمن تعديل البيانات الشخصية بطريقة تجعل من الممكن تمييز الأفراد في مجموعة بيانات باستخدام معرف فريد مثل رقم الهوية، أو خوارزميات التجزئة، مع حفظ بياناتهم الشخصية على حدة لأغراض فحص الجودة (انظر السؤال رقم (9)).

عند استخدام هذه التقنيات، ينبغي على الباحثين الرجوع إلى القوانين المحلية الوطنية ولوائح الرقابة الذاتية لتحديد العناصر التي يجب إزالتها لاستيفاء معيار إخفاء الهوية والهوية المستعارة لمثل هذه البيانات.

## 7 المصادر والمراجع

قوانين حماية البيانات العالمية، شركة DLA Piper

توجيهات EphMRA للإبلاغ عن الأحداث الضارة 2014

لائحة غرفة التجارة العالمية / جمعية "إيسومار" الدولية للأبحاث التسويقية والاجتماعية

دليل جمعية "إيسومار" لإجراء المقابلات مع الأطفال والشباب اليافعين

ISO 26362:2009 – مجموعات المشاركين المحتملين في الأبحاث التسويقية والأبحاث الاجتماعية واستطلاعات الرأي

ISO 20252 – للأبحاث التسويقية والأبحاث الاجتماعية واستطلاعات الرأي

مبادئ سياسة الخصوصية الصادرة عن منظمة التعاون الاقتصادي والتنمية

## 8 فريق المشروع

الرئيسان المشاركان:

- ريج بيكر، مستشار لجنة المعايير المهنية في جمعية "إيسومار" ومعهد البحوث التسويقية الدولي
- ديفيد ستارك، نائب الرئيس، النزاهة والامتثال والخصوصية، GfK

أعضاء فريق المشروع:

- دبرا هاردينغ، المدير التنفيذي لجمعية الأبحاث التسويقية
- ستيفن جِنك، مستشار
- كاثي جو، مدير المعايير الدولية والشؤون العامة، جمعية "إيسومار"
- وندر ماير، الرئيس التنفيذي للعمليات العالمية، MRops
- أشلين كويرك، المستشار العام في SSI
- باري ريان، مدير وحدة السياسات، جمعية الأبحاث التسويقية
- جين ڤان سوي، المدير، مجموعة واليس للاستشارات

تأتي جمعية "إيسومار" على رأس المؤسسات التي تهتم بتشجيع الأبحاث التسويقية وتطويرها والرفع من شأنها في جميع أنحاء العالم.

www.esomar.org