الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

مذكرة إرشادية حول

النظام الأوروبي لحماية البيانات الشخصية

١٤٤٠هـ / ٢٠١٩م

إشارة المشاركة: أبيض
تصنيف الوثيقة: متاح

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل او خارج المنشأة خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنيين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

حيث يمكنك مشاركتها مع آخرين من منشأتك أو منشأة أخرى على علاقة معكم أو بنفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

قائمة المحتويات

١. تمهيد ١

٢. معلومات أساسية ١

٣. مصطلحات أساسية في نظام حماية البيانات الأوروبي ٢

٤. تحديد قابلية تطبيق نظام حماية البيانات الأوروبي ٣

أ- قابلية تطبيق نظام حماية البيانات على الجهات التي لديها كيانات مؤسسة في الاتحاد الأوروبي ٣

ب-قابلية تطبيق نظام حماية البيانات على الجهات التي ليس لديها كيانات مؤسسة في الاتحاد الأوروبي ٤

٥. متطلبات نظام حماية البيانات الأوروبي ٦

٦. الخاتمة ١٣

١. تمهيد

في ضوء التطور الهائل الذي تتيحه التقنيات الحديثة، وخاصة فيما يتعلق بجمع البيانات الشخصية، ومعالجتها؛ و تحديد هوية الأشخاص وميولهم، وأطيافهم بشكل مباشر أو غير مباشر، ولما تمثله هذه البيانات الشخصية من أهمية؛ تعمل الكثير من الدول على توفير قوانين وتشريعات، تهدف إلى حماية حقوق مواطنيها، فيما يتعلق ببياناتهم الشخصية وخصوصيتها؛ ومن الأمثلة على ذلك، النظام الأوروبي لحماية البيانات الشخصية (The EU General Data Protection Regulation) والذي يرمز له اختصاراً بـ (GDPR).

يعد النظام الأوروبي لحماية البيانات الشخصية بمثابة التغيير الأكثر أهمية في تشريعات خصوصية وحماية البيانات الشخصية خلال العقدين الماضيين. ولما لهذا النظام من آثار قد تطال العديد من الأشخاص الطبيعيين أو المعنويين خارج حُدود الاتحاد الأوروبي؛ سعت الهيئة الوطنية للأمن السيبراني من خلال هذه المذكرة الإرشادية، إلى تقديم عرض مُجمل حول النظام الأوروبي لحماية البيانات الشخصية. وتتضمن هذه المذكرة إرشادات عامة؛ تساعد الجهات الحكومية والخاصة في تحديد مدى القابلية لتطبيق النظام الأوروبي لحماية البيانات الشخصية عليها، أو على بعض أنشطتها.

توضح هذه المذكرة -وبشكل مختصر وعام- الالتزامات المطلوبة من الجهات الحكومية والخاصة للامتثال للنظام الأوروبي لحماية البيانات، من خلال أمثلة متنوعة من الممارسات لبعض الجهات المحلية. مع الأخذ في الحسبان أن هذه المذكرة إرشادية؛ لا تُعد بأي حال من الأحوال استشارة قانونية.

٢. معلومات أساسية

تَهدف قوانين خصوصية البيانات في الاتحاد الأوروبي إلى منح الأفراد الصلاحية في التحكم في معلوماتهم الشخصية، بما في ذلك معرفة الجهة التي تقوم بجمعها، وكيفية استخدامها، وكذلك معرفة الجهات التي سيتم مشاركة البيانات معها.

بدأَ سريان نظام حماية البيانات في الاتحاد الأوروبي -رسميًا- في الخامس والعشرين من مايو ٢٠١٨ م. وسُنَّ هذا النظام وفقًا لقوانين الاتحاد الأوروبي التي كانت متبعة سابقًا؛ لا سيما توجيهات حماية البيانات (Data Protection Directive) التي أقرت في عام ١٩٩٥م، بهدف مواكبة التطور في المجال التقني.

يشمل النظام البيانات الشخصية لقاطني دول الاتحاد الأوروبي، وبغض النظر عن المكان الذي تعالج فيه تلك البيانات، سواءً كان ذلك داخل الاتحاد الأوروبي أو خارجه، ويَتضمن النظام عدة جوانب أكثر صرامة من القوانين والتوجيهات السابقة؛ كالالتزامات المتعلقة بالشفافية، والمساءلة، ووجوب الاحتفاظ بالسجلات التي تصف ممارسات الجهات المتعلقة بمعالجة البيانات الشخصية، ومتطلبات أخرى تتعلق بكيفية حماية البيانات الشخصية، وتمكين أصحاب البيانات من التحكم بها.

ينص النظام صراحةً على إمكانية تطبيقه خارج حدود الاتحاد الأوروبي، وذلك على الجهات التي تعالج بيانات شخصية لأفراد مقيمين في الاتحاد الأوروبي.

وسّع النظام صلاحيات الهيئات الأوروبية المختصة بحماية البيانات لتطبيق أحكام النظام، وفرض العقوبات على التجاوزات بأساليب متنوعة؛ تشمل غرامات طائلة تصل إلى عشرين مليون يورو، أو ٤٪ من حجم التعاملات السنوية للمنشأة المخالفة في جميع أنحاء العالم.

توصية: إن الأثر الهائل لنظام حماية البيانات الأوروبي لا يقتصر على الجهات الواقعة ضمن نطاق الاتحاد الأوروبي فحسب، وإنما يشمل أيضًا العديد من الجهات الواقعة خارج حدود الاتحاد الأوروبي. وقد يمتد هذا الأثر إلى الجهات القائمة في المملكة؛ إذ إن العديد منها يُعالج بيانات شخصية لأفراد مقيمين في الاتحاد الأوروبي، كالشركات ذات الجنسيات المتعددة، وشركات الخدمات المالية، ووكالات السفر والسياحة ووكالات التوظيف، وغيرها. ولهذا يتوجب على مثل هذه الجهات القيام بتقييم دقيق للأنشطة المتعلقة بمعالجة البيانات؛ لاتخاذ التدابير الكفيلة بعدم مخالفة هذا النظام، والحد من الوقوع تحت طائلته.

٣. مصطلحات أساسية في نظام حماية البيانات الأوروبي

يَعتمد نظام حماية البيانات الأوروبي على مصطلحات أساسية يتوجب فهمها ومراعاتها؛ وذلك تجنبًا للتعريفات والتفسيرات المختلفة المستخدمة في الأنظمة القانونية الأخرى. ولتيسير ذلك؛ تُسلط هذه المذكرة الإرشادية الضوءَ على أربعة مصطلحات أساسية، تُساعد على فهم نطاق تطبيق نظام حماية البيانات الأوروبي ومقتضياته:

البيانات الشخصية (Personal data): هي أي معلومات متعلقة بشخص طبيعي، سواء أكان معروفًا؛ أم يمكن التعرف عليه. والشخصُ الطبيعي الذي يمكن التعرف عليه هو الذي يمكن تحديده بشكل مباشر، أو غير مباشر؛ من خلال الرجوع إلى وسيلةٍ تُعرف بهويته مثل: الاسم، أو رقم الهوية، أو بيانات تحديد الموقع، أو مُعرف شخصي على شبكة الإنترنت أو أحد العوامل المُحددة للهُوية الجسدية، أو الفسيولوجية، أو الجينية، أو العقلية، أو الاقتصادية، أو الثقافية، أو الاجتماعية لذلك الشخص الطبيعي. ويطلق على الشخصي الطبيعي مسمى صاحب البيانات (Data subject).

المعالجة (Processing): هي عملية -أو مجموعة عمليات- تُنفذ على بيان شخصي، أو مجموعة بيانات شخصية (سواء أكان التنفيذ آليًّا أم غير آليٍّ) مثل: جمعها، أو تسجيلها، أو تنظيمها، أو هيكلتها، أو حفظها، أو تعديلها، أو تغييرها، أو استرجاعها، أو الاطلاع عليها، أو استخدامها، أو الكشف عنها؛ من خلال: بثّها، أو نشرها، أو جعلها متاحة، أو مواءمتها، أو دمجها، أو تقييدها، أو محوها وحذفها.

جهة التحكم بالبيانات (Controller): أي شخص طبيعي، أو اعتباري، أو جهة عامة، أو وكالة، أو هيئة أخرى تُحدد وحدها -أو مع أطراف أخرى- الأغراض من معالجة البيانات الشخصية، والوسائل اللازمة لذلك.

جهة معالجة البيانات (Processor): أي شخص طبيعي، أو اعتباري، أو جهة عامة، أو وكالة، أو هيئة أخرى تُعالج البيانات الشخصية، نيابةً عن جهة التحكم بالبيانات.

٤. تحديد قابلية تطبيق نظام حماية البيانات الأوروبي

تُراعى عدة معايير لتحديد مدى قابلية تطبيق نظام حماية البيانات الأوروبي على جهة ما. وعلى الرغم من أن النطاق الأساسي لتطبيق نظام حماية البيانات الأوربي، يتناول الجهات القائمة في أوروبا؛ إلا أن هنالك حالات تستدعي توسيع صلاحياته خارج حدود الاتحاد الأوروبي. ووفقاً لما دلت علية المادة الثالثة من النظام؛ حيث ينطبق في الحالات الآتية:

١. عمليات قائمة في الاتحاد الأوروبي، لمعالجة البيانات الشخصية في سياق أنشطة جهة تحكم بالبيانات؛ أو جهة معالجة للبيانات.

٢. عمليات معالجة البيانات الشخصية لأفراد متواجدين في الاتحاد الأوروبي؛ من قبل جهة تحكم بالبيانات، أو جهة معالجة للبيانات غير موجود في الاتحاد الأوروبي؛ وذلك عندما تكون أنشطة معالجة البيانات مرتبطة بـأحد أمرين:

أ. تقديم السلع أو الخدمات لأصحاب البيانات في الاتحاد الأوروبي؛ بصرف النظر عما إذا كان يَلزم من أصحاب البيانات تسديد مبلغ ما للحصول على تلك السلع أو الخدمات.

ب. رصد سلوكيات أصحاب البيانات، طالما أن هذه السلوكيات تحدث داخل الاتحاد الأوروبي.

أ- قابلية تطبيق نظام حماية البيانات على الجهات التي لديها كيانات مؤسسة في الاتحاد الأوروبي

تبين الفقرة (١) من المادة الثالثة من نظام حماية البيانات الأوروبي؛ إمكانية تطبيق النظام على بعض أنشطة معالجة البيانات، القائمة خارج الاتحاد الأوروبي؛ لأنها تندرج في إطار (نشاطات كيان مؤسس في الاتحاد الأوروبي تابع لجهة التحكم أو لجهة معالجة البيانات).

وتُفسر محاكم الاتحاد الأوروبي مصطلح كيان مؤسس (establishment) بصفته مفهومًا واسعًا ومرنًا، لا يرتبط بأي صيغة قانونية محددة. أي أن جهة ما قد تعد كيانًا مؤسسًا في الاتحاد الأوروبي؛ إذا كانت تمارس أي نشاط حقيقي وفعّال، عبر ترتيبات مستقرة وثابتة (stable arrangement) في الاتحاد الأوروبي؛ حتى وإن كان هذا النشاط محدوداً. فقد قررت محكمة العدل الأوروبية في إحدى القضايا المعروفة، أن وجود ممثل وحيد قد يكون كافيًا لتعد جهة ما؛ كيانًا مؤسساً في الاتحاد الأوروبي، ما دامت تتوافر فيها عوامل أخرى (مثل: موقع إلكتروني مُخصّص للعملاء المحليين، أو استخدام لغة محلية أوروبية، أو عنوان محلي) والتي قد تستوفي -مجتمعة- الحد الأدنى من متطلبات ممارسة نشاط حقيقي وفعّال؛ من خلال ترتيبات مستقرة وثابتة.

أما فيما يتعلق بعبارة في إطار نشاطات (in the framework of activities) فإن صياغة الفقرة (١) من المادة الثالثة غيرُ جديدة على الإطلاق؛ فقد وردت مسبقًا ضمن تشريعات حماية البيانات والخصوصية وقواعدها السابقة في الاتحاد الأوروبي، كما استخدمتها المحاكم والهيئات التنظيمية للخصوصية وحماية البيانات؛ من أجل توسيع نطاق أحكام الخصوصية، وحماية البيانات للاتحاد الأوروبي؛ لتشمل أنشطة المنشآت غير القائمة في الاتحاد الأوروبي، ولكن لها كيانات مؤسسة فيه. ففي حال وجود صلة حقيقية بين عمليات

معالجة البيانات الخاصة بكيان مؤسس خارج الاتحاد الأوروبي، وبين نشاطات كيان مؤسس داخله؛ فإن هذه العمليات تخضع لنظام حماية البيانات الأوروبي، حتى وإن كان الكيان المؤسس داخل الاتحاد الأوروبي لا يعالج البيانات بنفسه.

تتضمن الفقرة (٢) من المادة الثالثة من نظام حماية البيانات الأوروبي حكمًا يمتد تطبيقه إلى خارج النطاق الإقليمي للاتحاد (سوف ترد مناقشته في القسم اللاحق) ولهذا السبب قد لا تعتمد المحاكم والهيئات التنظيمية للخصوصية وحماية البيانات؛ اعتمادًا كبيرًا على قاعدة (في إطار نشاطات) التي تنص عليها الفقرة (١) من المادة الثالثة؛ لإثبات سريان نظام حماية البيانات على المنشآت القائمة خارج الاتحاد الأوروبي. وعلى الرغم من ذلك، تُقدم الفقرة (١) من المادة الثالثة حال أخرى؛ في إمكانية تطبيق نظام حماية البيانات الأوروبي على بعض أنشطة معالجة البيانات، من قبل جهات خارج الاتحاد الأوروبي؛ وذلك بسبب الرابط الموجود بين هذه الجهات، وبين كيانات مؤسسة في الاتحاد الأوروبي.

ب- قابلية تطبيق نظام حماية البيانات على الجهات التي ليس لديها كيانات مؤسسة في الاتحاد الأوروبي

تتضمن الفقرة (٢) من المادة الثالثة أكثر المواد القانونية أهمية للجهات في المملكة؛ لتحديد مدى قابلية تطبيق نظام حماية البيانات الأوروبي على تلك الجهات. وحسب الفقرة (٢) من المادة الثالثة، فإن نظام حماية البيانات الأوروبي ينطبق على جهة ما؛ في إحدى حالين هما:

أ. تقديم السلع أو الخدمات للمقيمين في الاتحاد الأوروبي.

ب. مراقبة سُلوكيات المقيمين في الاتحاد الأوروبي؛ (لتحديد الأنماط الشخصية Profiling).

ويمكن القولُ بأن الأمر يتطلب تحليلاً دقيقًا للوقائع والظروف المحيطة بها؛ وذلك لمعرفة كيفية تطبيق الفقرة (٢) من المادة الثالثة على الجهات القائمة خارج نطاق الاتحاد الأوروبي.

١- تقديم السلع أو الخدمات للمقيمين في الاتحاد الأوروبي

من أجل تحديد المقصود بعبارة (تقديم السلع أو الخدمات) للمقيمين الأوروبيين ضمن الفقرة (٢/أ) من المادة الثالثة؛ يجب مراجعة الحيثية القانونية الثالثة والعشرين من نظام حماية البيانات الأوروبي، والتي تنص على أنه "ينبغي التحقق من وضوح نيّة جهة التحكم، أو جهة معالجة البيانات في تقديم الخدمات، لأصحاب البيانات المقيمين في إحدى الدول الأعضاء في الاتحاد الأوروبي". ويعني هذا؛ وجود النية الواضحة الجليّة لممارسة نشاط تجاري، موجه إلى الأفراد المقيمين في الاتحاد الأوروبي. وتَستطرد الحيثية القانونية الثالثة والعشرون بالحديث عن ضرورة إجراء دراسة متعددة الجوانب من أجل التحقق من وجود النية من عدمها، إذ إن مجرد إنشاء موقع إلكتروني مخصص للمستخدمين الأوروبيين -على سبيل المثال- ليس كافيًا بذاته؛ لاستيفاء الحد الأدنى من شروط كون السلع، أو الخدمات، مقدمة إلى المقيمين الأوروبيين. لكن وجود عوامل

أخرى كاستخدام عدة لغات أوروبية، أو إتاحة إمكانية طلب المنتجات بتلك اللغات، أو استخدام عملة أوروبية، أو الإشارة إلى "العملاء الأوروبيين"؛ قد يؤكد وجود النية الكافية لممارسة نشاط تجاري في الاتحاد الأوروبي. وقد نظرت المحاكم الأوروبية في هذه المسألة؛ فذكرت مجموعة من المعايير، التي يمكنها المساعدة في تحديد مدى وجود نية طرف ما، لممارسة نشاط تجاري في أوروبا من عدمه، ومن أمثلة هذه المعايير:

- وجود بيان صريح، يشير إلى أن الخدمة المقدمة تستهدف فعلًا المستخدمين الأوروبيين.
- التعاقد مع أحد محركات البحث الإلكترونية؛ من أجل فهرسة الموقع الإلكتروني، فهرسةً تسهل وصول العملاء الأوروبيين إليه.
- الإشارة -على الموقع الإلكتروني أو في المواد الدعائية- إلى تقديم خدمات عالمية، ولجميع العملاء من جميع أنحاء العالم.
- نشر أرقام اتصال دولية، أو استخدام نطاقات للمواقع الإلكترونية (مثل: النطاق الأوروبي (.eu) أو النطاق الفرنسي (.fr) أو النطاق الدنماركي (.de)) مختلفة عن النطاق الخاص بالبلد الأصلي لمزود الخدمة الذي يقع خارج الاتحاد الأوروبي.

توصية: تجدر الإشارة إلى أهمية دراسة كل حال على حدة، من أجل تحديد مدى انطباق الحد الأدنى من الشروط المنصوص عليها في الفقرة (٢/أ) من المادة الثالثة على نشاطات منظمات، أو منشآت تجارية معينة.

٢- رصد سلوكيات المقيمين في الاتحاد الأوروبي

تبين الحيثية القانونية الرابعة والعشرون من النظام عن مقصد المشرعين الأوروبيين من مفهوم رصد سلوكيات (Monitoring the behavior) المقيمين الأوروبيين، الواردة في الفقرة (٢/ب) من المادة الثالثة؛ حيث نَصت على انه "ينبغي التحقق من مدى رصد سلوكيات الأشخاص الطبيعيين على الإنترنت؛ بما في ذلك تحديد نمط شخصية الشخص الطبيعي؛ لا سيما إذا كان ذلك من أجل اتخاذ قرارات تتعلق به، أو من أجل تحليل شخصيته، أو توقع تفضيلاته، أو سلوكياته، أو توجهاته".

وتشير الأمثلة الموضحة في الحيثية القانونية إلى أن المقصود برصد السلوكيات، في هذا السياق هو الرصد ذو النطاق الواسع لسلوكيات الأشخاص بهدف التأثير عليهم؛ اعتمادًا على تحليل تفضيلاتهم الشخصية والتنبؤ بها. ولكن يجدر الإشارة هنا، إلى أن هذا النوع من الرصد ذي النطاق الواسع لسلوكيات الأشخاص؛ هو أمر شائع في عصرنا هذا، خاصة مع الانتشار الواسع لشبكات الإعلانات الرقمية وأدواتها على الإنترنت، والتي توفر وسائل متنوعة لتعقب مستخدمي المواقع الإلكترونية، واستهدافهم بمحتوى معين.

توصية: ينبغي تسليط الضوء على أن مبدأ (رصد السلوكيات) الوارد في الحيثية القانونية الرابعة والعشرين، لا يتطلب نية واضحة لرصد سلوكيات الأفراد المقيمين في الاتحاد الأوروبي، وهذا على عكس ما ورد سابقًا في الحيثية القانونية الثالثة والعشرين؛ فيما يتعلق بضرورة وضوح النية لممارسة نشاط تجاري مع المقيمين في الاتحاد الأوروبي. ويعد العامل الرئيس -في هذه الحال- كون الغرض من عملية جمع المعلومات الشخصية؛

هو رصد سلوكيات الأفراد المقيمين في الاتحاد الأوروبي والتأثير عليهم. وعلى هذا يكون احتمال تعرض مستخدمين أوروبيين، لممارسات رصد السلوكيات؛ كافياً لانطباق نظام حماية البيانات الأوروبي على هذه الممارسات.

٥. متطلبات نظام حماية البيانات الأوروبي

عندما تصل جهة ما إلى نتيجة مفادها انطباق نظام حماية البيانات الأوروبي عليها، أو على بعض أنشطتها؛ فيجب على هذه الجهة أن تقوم بجميع الخطوات المطلوبة، لضمان التزامها بمتطلبات النظام وامتثالها لشروطه. وقد تشمل هذه الخطوات الاستعانة بمستشار قانوني، أو خبير استشاري في حماية البيانات الشخصية، أو عقد ورش عمل، واجتماعات داخلية، مع الأطراف ذات العلاقة، أو إجراء تقييم أولي لمعرفة الأثر الفعلي والمباشر لنظام حماية البيانات الأوروبي على النشاطات اليومية لهذه الجهة.

ويُقدم هذا القسم توضيحا عاماً -دون الدخول في التفاصيل- لمتطلبات نظام حماية البيانات الأوروبي. مع التذكير بأن هذه المذكرة إرشادية، ولا تعد بأي حال من الأحوال استشارة قانونية.

أ- لمحة عن مبادئ معالجة البيانات

أشارت المادة الخامسة من نظام حماية البيانات الأوروبي إلى ما يُعرف بـمبادئ معالجة البيانات (Data processing principles) وهي المفاهيم الأساسية التي بُني عليها نظام حماية البيانات الأوروبي، والتي تَرسم الإطار العام لفهم كيفية الالتزام بالنظام، والامتثال لشروطه. وهذه المبادئ هي:

(١) المشروعية (lawfulness)، والعدالة (fairness)، والشفافية (transparency).

(٢) حصر الغرض من معالجة البيانات (purpose limitation).

(٣) جمع الحد الأدنى من البيانات (data minimization).

(٤) دقة البيانات (data accuracy).

(٥) تخزين البيانات لمدة محدودة (storage limitation).

(٦) سلامة البيانات (integrity) وسريتها (confidentiality).

(٧) المساءلة (accountability).

وفيما يلي نناقش هذه المبادئ بشيء من التفصيل، مع الأخذ في الحسبان الجوانب العملية لها.

ب- المشروعية والعدالة والشفافية

المسوغ النظامي (Legal basis): ينص نظام حماية البيانات الأوروبي، على عدم جواز استخدام البيانات الشخصية؛ إلا لأغراض مشروعة، مبنية على مسوغ نظامي محدد. وتشير المادة السادسة من النظام إلى ستة مسوغات نظامية تتيح لجهة التحكم بالبيانات، جمع البيانات الشخصية ومعالجتها:

(١) بناء على موافقة صاحب البيانات.

(٢) لإعداد عقد، أو لاستيفاء شروطه.

(٣) للامتثال لمتطلبات قانونية.

(٤) لحماية المصالح الحيوية لصاحب البيانات.

(٥) لتنفيذ مهمة للصالح العام، أو ممارسة واجب قانوني.

(٦) لتحقيق مصالح مشروعة لجهة التحكم بالبيانات؛ بشرط ألا تتجاوز حقوق متعلقة بخصوصية البيانات الشخصية أو تنتهكها.

ولذلك فلابد من توفر أحد هذه المسوغات النظامية الستة؛ عند قيام جهة التحكم بالبيانات، بجَمع أي بيانات شخصية، أو استخدامها.

موافقة صاحب البيانات (Consent): لموافقة صاحب البيانات الواردة في النظام؛ مفهوم محدد، يتطلب استيفاء معايير أساسية محددة؛ تتمثل في كون موافقة الفرد على معالجة بياناته طوعًا، وصريحةً، ومحددة، وعن دراية تامة؛ دون وجود أي لَبْسٍ على الإطلاق (أي أن الموافقة لا تتم إلا بالإيجاب والقبول الصريحين) وللفرد الحق في التراجع عن موافقته على جمع ومعالجة البيانات، عندما يريد ذلك؛ على أن يكون التراجع عن الموافقة على معالجة البيانات الشخصية في مثل سهولة موافقة صاحب البيانات على جمعها ومعالجتها. مع العلم أن معايير موافقة صاحب البيانات لا تستوفى؛ عندما يقوم صاحب البيانات بالموافقة الصامتة، وكذلك لا تستوفى هذه المعايير في حال غياب الرد الواضح الصريح، سواءً أكان ذلك سلباً أم إيجاباً.

إشعار الخصوصية (Privacy notice): يشير مبدأ الشفافية -الذي سبقت الإشارة إليه بوصفه أحد المبادئ لمعالجة البيانات- إلى توفير معلومات محددة للأفراد، عن كيفية جمع بياناتهم الشخصية، واستخدامها، ومشاركتها، وتخزينها، والتخلص منها في نهاية المطاف؛ ووفقًا لأي أسس نظامية يتم كل ذلك. وتُقدم هذه المعلومات عادة على هيئة إشعار خصوصية، يتاحُ للأفراد قبل جمع أي بيانات عنهم أو معالجتها. كما يجب أن يُحدد إشعار الخصوصية جهة التحكم بالبيانات (متضمنًا وسيلة الاتصال بها). ويوضحُ حقوق الأفراد فيما يتعلق ببياناتهم، ويفسر أي عملية معالجة قد تؤثر عليهم وغيرها من المعلومات.

ويؤكد نظام حماية البيانات الأوروبي بشدة على ضرورة تقديم هذه المعلومات للأفراد، بأسلوب يسهل الوصول إليه؛ وذلك باستخدام لغة بسيطة وواضحة، مع إتاحة الوسائل المناسبة للأفراد، من أجل طلب أي معلومات إضافية، أو ممارسة حقوقهم التي كفلها النظام.

ج- حصر الغرض من جمع البيانات

عند جمع بيانات لغرض معين؛ لا يجوز استخدامها لأغراض أخرى تتعدى الغرض الأساسي أو لا تتوافق معه. ويرتبط هذا الاشتراط بشكل مباشر، بمبدأ الشفافية؛ لأن أيّ عملية إضافية لمعالجة البيانات الشخصية، لأغراض أخرى، تتعدى الغرض الأساسي؛ تتطلب إشعار أصحاب البيانات بهذه الأغراض الجديدة لمعالجة بياناتهم،

ومنحهم الفرصة للاعتراض أو الموافقة عليها، وممارسة حقوقهم المشروعة الأخرى المتعلقة بجمع بياناتهم الشخصية ومعالجتها.

د- جمع البيانات بالحد الأدنى، وتخزينها لمدة محدودة

جمع البيانات بالحد الأدنى: يتعين على جهة التحكم بالبيانات جمع أقل قدر ممكن من البيانات الشخصية اللازمة؛ لتحقيق الغرض الأساسي من جمع البيانات. ويتضح -عند ربط هذا المبدأ بمفهوم حصر الغرض من جمع البيانات- أن تحقيق الحد من جمع البيانات؛ يتطلب قيام جهة التحكم بالبيانات بالتأني والتأمل قبل القيام بجمع البيانات الشخصية؛ لأن جمع بيانات شخصية أكثر من المطلوب، قد يعد انتهاكًا للخصوصية؛ ويمكن أن يُعرض البيانات الإضافية التي تم جمعها لأنواع مختلفة من المخاطر. وهذا يعني أن مبدأ جمع البيانات بالحد الأدنى؛ يتطلب تحديد البيانات الشخصية المطلوب جمعها بصورة دقيقة جدًّا.

تخزين البيانات لمدة محدودة: إن مبدأ تخزين البيانات لمدة محدودة، يقضي بعدم جواز الاحتفاظ بالبيانات الشخصية، إلا للفترة الزمنية اللازمة؛ لتحقيق الغرض الأساسي الذي جمعت له. ويتعين بعد تحقق هذا الغرض حذف تلك البيانات، أو إخفاء هوية صاحبها؛ بحيث لا يمكن ربط تلك البيانات بالفرد نفسه من جديد. وهذا من شأنه أن يلقي العبء -مرة أخرى- على جهة التحكم بالبيانات، وجهة معالجة البيانات؛ للقيام بمراجعة دقيقة لممارساتهم، المتعلقة بتخزين البيانات؛ من أجل التحقق من عدم الاحتفاظ بالبيانات شخصية لفترة أطول من اللازم. ويتطلب القيام بهذا الأمر-عادة- اتباع جداول زمنية للاحتفاظ بالبيانات تتصف بالآتي:

أ. الاتساق مع قوانين الاحتفاظ بالبيانات وشروطها المعمول بها؛ والتي غالبًا ما تكون مختلفة حسب القطاع الذي تنتمي له البيانات (من مثل، شروط الاحتفاظ بالبيانات المتعلقة القطاع المالي).

ب. الاتفاق عليها بين جميع الأطراف ذات العلاقة، داخل جهة التحكم بالبيانات، أو جهة معالجة البيانات.

ت. القابلية للتنفيذ بشكل معقول ومنضبط.

ويرتبط هذا الأمر أيضاً بمبدأ الشفافية؛ من حيث وجوب إشعار الفرد، عن مدة الاحتفاظ بالبيانات، بصفة عامة، وذلك قبل جمع بياناته؛ بما في ذلك المسوغات القانونية ذات الصلة (أي المتوافقة مع قوانين الاحتفاظ بالبيانات المعمول بها) التي تُلزم جهة التحكم بالبيانات، بالاحتفاظ بسجلات البيانات الشخصية لفترة زمنية، تمتد إلى ما بعد انتفاء الغرض الأساس من جمع البيانات الشخصية ومعالجتها.

هـ- أمن البيانات ودقتها وسريتها وسلامتها

لا يقتصر النظام على خصوصية المعلومات فحسب؛ وإنما يعنى بمسألة حماية البيانات الشخصية أيضًا، مما يعني أنه يقع على عاتق جهة التحكم بالبيانات، وجهة معالجة البيانات؛ مسؤولية ضمان دقة المعلومات وسلامتها، والتعامل معها بسرية تامة، واتخاذ التدابير التنظيمية، والتقنية المناسبة، التي تكفل الحماية

للبيانات.

تدابير حماية البيانات: يجب على جهة التحكم بالبيانات وجهة معالجة البيانات على حد سواء؛ مراجعة الممارسات الأمنية المستخدمة، وتحديثها بانتظام؛ حيث لا يُقدم النظام إلا توجيهات عامة في هذا الصدد؛ إذ ينص على وجوب مراعاة تدابير حماية البيانات لـ "أحدث تقنيات معالجة البيانات، وطبيعتها، وتكاليف تنفيذها، ونطاقها، وسياقها، وأغراضها؛ إضافة إلى مراعاة جميع المخاطر (على الأفراد الذين يتم معالجة بياناتهم)". ثم يسرد النظام قائمة من التدابير المحددة (مثل: استخدام الأسماء المستعارة (pseudonymization)، والتشفير، والبرتوكولات الأمنية، واختبارات دورية للضوابط) التي قد تكون كافيةً بحد ذاتها، أو على أقل تقدير جزءًا من استراتيجية حماية البيانات وتقليل المخاطر عليها.

تسرب البيانات (Data breaches): يتميز النظام بأنه دقيق للغاية فيما يتعلق بحوادث تسرب البيانات؛ إذ يفرض على جهة التحكم بالبيانات إخطار الهيئات المختصة بحماية البيانات، عن حوادث تسرب البيانات، وذلك خلال اثنان وسبعين ساعة من اكتشافها؛ ويجب على جهات التحكم بالبيانات -في بعض الأحوال- إشعار الأفراد المتضررين أيضًا. وقد يشكل الإخطار عن حوادث تسرب البيانات تحديًا تشغيليًا للعديد من الجهات. ولا يقتصر هذا الأمر على جهات التحكم بالبيانات فحسب، وإنما يشمل جهات معالجة البيانات أيضًا؛ فهم المسؤولون عن إخطار جهة التحكم بالبيانات عن أي عملية تسرب للبيانات، دون أي تأخير لا مبرر له.

توصية: من الضروري وضع خطة استجابة فعالة لحوادث تسرب البيانات، واتباع إستراتيجية دقيقة جدًا للأمن السيبراني، والتنسيق، والتواصل بمستوى رفيع بين الأطراف ذات العلاقة، داخل جهة التحكم بالبيانات، أو جهة معالجة البيانات؛ وامتلاك القدرة على الاستجابة السريعة عند إفشاء البيانات الشخصية، أو تعديلها، أو ضياعها، أو إتلافها عمدًا، أو عن غير قصد. ويجب على الجهات التي تقع تحت نطاق تطبيق النظام؛ صياغة خطة استجابة لحالات تسرب البيانات، بحيث تشمل -على سبيل المثال لا الحصر: المسؤوليات، والمهمات المحددة، والمعايير الخاصة بتحديد ماهية حوادث تسرب البيانات، والقنوات المخصصة للتبليغ عن حوادث تسرب البيانات.

و- حقوق أصحاب البيانات

إشعار الخصوصية (Privacy notice): يضمن النظام حقوقًا محددةً لأصحاب البيانات؛ لتمكينهم من التحكم في بياناتهم الشخصية. وتشمل هذه الحقوق كما سبق ذكره؛ إخطارهم قبل معالجة البيانات، وتزويدهم بمعلومات محددة (عادة ما يكون على شكل إشعار الخصوصية أو سياستها) عن كيفية جمع البيانات، واستخدامها، ومشاركتها، وتخزينها، والتخلص منها. وإذا لم يمكن تقديم هذه المعلومات -عند جمعها- فيجب إتاحتها لاحقًا في أقرب وقت ممكن.

الحقوق المرتبطة بالبيانات الشخصية (Personal data rights): بمجرد إخطار الفرد قبل معالجة البيانات، وتزويده بالمعلومات اللازمة (وفي بعض الحالات طلب موافقته على شروط إشعار الخصوصية) يمكن عندها جمع البيانات واستخدامها. كما يتمتع الفرد عندها بمطلق الحرية في ممارسة حقوقه المرتبطة بالبيانات بما في

ذلك الحقوق الآتية:

(١) الوصول للبيانات الشخصية.

(٢) تصحيح المعلومات غير الدقيقة والقديمة.

(٣) حذف البيانات الشخصية.

(٤) الحد من معالجة البيانات الشخصية.

(٥) الاعتراض على أنواع محددة من معالجة البيانات.

(٦) الإخطار عن القرارات التي يتم اتخاذها آليا (automated decision-making) بناء على معالجة لبياناته الشخصية.

(٧) الإبلاغ عن حوادث تسرب البيانات، التي تشكل خطرًا شديدًا على حقوق الفرد وحرياته.

ويتعين على جهة التحكم بالبيانات تسهيل إجراءات ممارسة هذه الحقوق، والرد على طلبات الأفراد؛ خلال شهر واحد من تقديمها. كما يجب إبلاغ الأفراد عند اتخاذ أي إجراء يتعلق بتنفيذ طلبهم؛ إضافة إلى تقديم جهة التحكم بالبيانات تفسيرًا واضحًا عند رفض أيّ طلب.

تسهيل ممارسة الحقوق (Facilitation of Rights): على غرار المتطلبات الأخرى في نظام حماية البيانات الأوروبي؛ بما يقتضي تسهيل استيفاء حقوق أصحاب البيانات من الجهات، في تحديد إجراءات واضحة، خاصة باستقبال الطلبات المتعلقة بهذه الحقوق؛ ومن ثم تقييمها، والرد عليها، ومعالجتها. وقد تتداخل حقوق معينة بعضها مع بعض؛ مثل: تداخل حق حذف البيانات الشخصية، مع متطلبات أخرى (مثل قوانين استعادة البيانات التي يمكن تطبيقها) وهو ما يتطلب دراستها مسبقًا؛ ومن ثم معالجة هذا التداخل، وفق خطة عمل لتقديم تفسير للفرد المعني.

ز- عمليات نقل البيانات الدولية

عند نقل بيانات شخصية بين جهة التحكم بالبيانات، وجهة معالجة البيانات خاضعتان للنظام؛ فلابد من إبرام اتفاقية معالجة البيانات، من أجل تحديد التزامات كل من الطرفين؛ لضمان وجود تدابير وقائية مناسبة لحماية تلك البيانات.

الآليات المشروعة لنقل البيانات خارج الاتحاد الأوروبي (Transfer mechanism options): يتعين عند نقل بيانات شخصية -خارج الاتحاد الأوربي- أن تتوفر لهذه البيانات الحماية المطلوبة؛ وفقا لأحكام النظام، وذلك بتبني آلية مشروعة من آليات نقل البيانات خارج الاتحاد الأوروبي. ويقرر النظام عدة آليات يمكن لجهة التحكم بالبيانات استخدامها، لنقل البيانات الشخصية خارج الاتحاد الأوروبي، فعلى سبيل المثال: توجد قائمة من البلدان التي يعترف الاتحاد الأوروبي بقدرتها على توفير المستوى المناسب لحماية البيانات؛ وهو ما يتيح حرية حركة البيانات الشخصية بين الاتحاد، وتلك البلدان. كما توجد اتفاقات وأُطر خاصة بين بعض تلك البلدان والاتحاد الأوروبي؛ تسمح بنقل البيانات، وفقاً لشروط معينة (مثل: اتفاقية درع الخصوصية (Privacy

shield) المبرمة بين دول الاتحاد الأوروبي والولايات المتحدة الأمريكية). ويتوافر أيضًا خيار آخر يُعرف بالقواعد الإلزامية للشركات (Binding Corporate Rules) وهي مجموعة محددة من التزامات خصوصية البيانات؛ تُوافق على الامتثال لها، الشركات ذات الجنسيات المتعددة؛ فتصبح مُلزمة قانوناً بتنفيذ متطلباتها. ويتيح هذا النوع من القواعد الإلزامية (بعد إقرارها من قبل الهيئات التنظيمية للخصوصية في الاتحاد الأوروبي) حرية انتقال البيانات الشخصية بين كيانات الشركة في مختلف دول العالم، في حال موافقتها على الالتزام بـتلك القواعد.

بنود الاتحاد الأوروبي النموذجية (EU model clauses): إن الآلية الأكثر استخدامًا في الواقع العملي لنقل البيانات خارج الاتحاد الأوروبي؛ هي اتفاقية نقل البيانات بين جهة التحكم بالبيانات، وجهة معالجة البيانات. وعادة ما تستند هذه الاتفاقيات إلى بنود نموذجية أقرها الاتحاد الأوروبي، والتي تنص على التزامات واجبة التنفيذ؛ ينبغي على جهة التحكم بالبيانات، وجهة معالجة البيانات، الاتفاق عليها، قبل الشروع في نقل أي من البيانات إلى جهة معالجة البيانات. وتلزم هذه البنود النموذجية جهة معالجة البيانات بما يأتي:

أ. عدم استخدام البيانات الشخصية، إلا لأغراض محددة؛ وفقًا لتعليمات جهة التحكم بالبيانات.

ب. توفير تدابير خاصة لحماية البيانات، ومنع تسريبها؛ وتسهيل ممارسة الحقوق المرتبطة بالبيانات الشخصية.

ت. يجب أن تشمل أي تعاقدات لاحقة، تقوم بها جهة معالجة البيانات مع جهات أخرى، على التزامات مشابهة؛ قبل أن تتلقى تلك الجهات البيانات الشخصية.

ث. حذف البيانات، أو إعادتها لجهة التحكم بالبيانات؛ في حال تحقق الغرض منها.

ومما يجدر ذكره؛ أن هذا النوع من اتفاقيات نقل البيانات، يمنح جهة التحكم بالبيانات، الحق في تدقيق عمل جهة معالجة البيانات، والتأكد من امتثالها لهذه الالتزامات، ومساءلتها في حال عدم الامتثال. كما تعطي هذه البنود النموذجية الحق لصاحب البيانات -بوصفه طرفاً ثالثاً مستفيدًا (Third Party Beneficiary)- في مساءلة جهة معالجة البيانات.

توصية: تنطوي عملية تحديد آلية النقل المناسبة، على تحليل دقيق للأطراف المشاركة، والبيانات المعنية، والحقائق والظروف المحيطة. فيجب على الجهات التي ينطبق عليها النظام -سواء أكانت جهة التحكم بالبيانات أم جهة معالجة البيانات- مراجعة حركة نقل البيانات الخاصة بها، وضمان استخدامات تلك الجهات آلية نقل مشروعة، وفقاً لأحكام النظام الأوروبي.

ح- إدارة شؤون مقدمي خدمات المعالجة

يفرض النظام على جهة التحكم بالبيانات، ثلاثة التزامات رئيسة؛ تتعلق بمقدمي خدمات المعالجة تتمثل في التالي:

أ. الحرص على اختيار جهات معالجة البيانات ذات الكفاءة العالية.

ب. تدوين شروط معالجة البيانات في اتفاقية مكتوبة.

ت. استخدام آلية مشروعة عند نقل البيانات دولياً.

الحرص على اختيار جهات معالجة البيانات ذات الكفاءة العالية (Due diligence): يُلزم أحد المتطلبات جهة التحكم بالبيانات، بعدم التعامل مع أي من جهات المعالجة للبيانات، إلا عند اتخاذه التدابير التنظيمية والتقنية المناسبة؛ التي تستوفي متطلبات النظام. وقد يستلزم هذا الأمر إجراء استقصاءات مطولة قبل التعاقد مع مقدم خدمات المعالجة، ومن ثم متابعة مدى امتثاله لنظام حماية البيانات بشكل دوري أثناء التعاقد معه. وعند نهاية فترة التعاقد؛ يتوجب ضمان تخلص مقدم خدمات المعالجة من تلك البيانات بالطريقة المناسبة والآمنة، أو نقلها إلى جهة التحكم بالبيانات.

شروط معالجة البيانات (Data processing terms): يجب إبرام اتفاقية معالجة البيانات مع أي مقدم خدمات المعالجة. ويجب أن تنطوي هذه الاتفاقية على التزامات معينة؛ وردت في المادة الثامنة والعشرين من نظام حماية البيانات الأوروبي، ويتوجب على جهة معالجة البيانات التقيد بها؛ وتتمثل هذه الالتزامات في التالي:

أ. عدم استخدام البيانات، إلا وفقًا لتعليمات جهة التحكم بالبيانات.

ب. وضع التدابير الخاصة للحفاظ على البيانات وحمايتها.

ت. مساعدة جهة التحكم بالبيانات في الرد على طلبات الأفراد.

ث. اشتمال أي تعاقدات لاحقة تقوم بها جهة معالجة البيانات، مع جهات أخرى على التزامات مشابهة قبل أن تتلقى تلك الجهات البيانات الشخصية.

ويستمر سريان اتفاقية معالجة البيانات هذه، طيلة فترة العلاقة مع مقدم خدمات المعالجة، ويتعين بعد ذلك حذف البيانات، أو إعادتها لجهة التحكم بالبيانات.

آلية نقل البيانات خارج الاتحاد الأوروبي: يلزم توفر آلية مشروعة لأي عملية نقل دولية للبيانات الشخصية. وتتوفر العديد من آليات نقل البيانات، وذلك وفقًا لكل حالة، وبحسب البلدان المعنية. على أن أكثر الخيارات شيوعا هي (البنود النموذجية) التي أقرها الاتحاد الأوروبي. ومن الناحية العملية؛ فإنه غالبًا ما تُدمج هذه البنود مع اتفاقية معالجة البيانات المذكورة سلفًا.

ط- المساءلة

ينطوي نظام حماية البيانات الأوروبي على أحكام مساءلة شاملة؛ لا تقتصر على منح هيئات حماية البيانات في الاتحاد الأوروبي، سلطات ذات نطاق واسع؛ لتطبيق النظام، وفرض غرامات مالية في حال عدم الامتثال له؛ بل تشمل التزامات الحوكمة الداخلية والتوثيق؛ التي ينبغي على جهات التحكم بالبيانات وجهات معالجة البيانات اتباعها بدقة.

مسؤول حماية البيانات (Data protection officer): يتعين على بعض الجهات، تعيين مسؤول حماية البيانات وهو المسؤول عن الإشراف على التزام المنشأة بنظام حماية البيانات الأوروبي. ويؤدي المسؤول مهمة التواصل والتنسيق مع أصحاب البيانات، وكذلك مع الهيئات المختصة بحماية البيانات؛ كما يجب عليه تأدية

واجبات متنوعة، تتراوح ما بين النواحي الإدارية والتشغيلية، وتقديم الاستشارات.

السياسات والإجراءات والتدريب (Policies, procedures and training): يتعين على الجهات تطبيق سياسات وإجراءات داخلية، تُحدد بوضوح كيفية الوفاء بالتزامات النظام من الناحية العملية. كما يجب أيضًا الالتزام بتطبيق مبدأ الخصوصية بالتصميم وبالافتراض (Privacy by design and by default) وهذا يعني ضرورة قيام الجهات بالنظر في خصوصية البيانات، أثناء تصميم منتج جديد، أو إجراء جديد؛ ومن ثم إدماج وسائل الحماية التي تضمن سلامة البيانات الشخصية، طوال دورة حياة تلك البيانات، كما يتعين على الجهات؛ ضمان خضوع موظفيها لالتزامات مناسبة، من أجل احترام سرية البيانات الشخصية، إضافة إلى تدريب الموظفين على متطلبات نظام حماية البيانات الأوروبي؛ بما في ذلك كيفية تأثيره على أنشطتهم اليومية، إلى جانب توفير الإرشادات الخاصة بمهمة كل منهم، عند الحاجة لذلك.

التوثيق (Documentation): يعد التوثيق من الأمور المرتبطة بمبدأ الشفافية، وينص على وجوب احتفاظ الجهات بصفة عامة على سجلات داخلية مفصلة عن حركة البيانات الشخصية، ضمن ما يسمى سجل معالجة البيانات (data processing register). وقد يتعين على الجهات أيضًا تقييم أثر حماية البيانات (data protection impact assessment) عند معالجتها بيانات شخصية حساسة، أو في حال إمكانية تعرض بيانات شخصية لمخاطر عالية، أثناء معالجتها. ويتضمن ذلك تقييم المخاطر على البيانات الشخصية، وتحديد الثغرات، واقتراح تدابير تخفف من هذه المخاطر على تلك البيانات.

٦. الخاتمة

تعد المعلومات الواردة في هذه المذكرة الإرشادية مرجعًا للجهات الحكومية، والخاصة القائمة في المملكة؛ من أجل تعزيز الوعي بنظام حماية البيانات الأوروبي. ونوصي بشدة أن تقوم هذه الجهات بمراجعة دقيقة لتلك المتطلبات، والتماس المشورة عند الضرورة؛ للتحقق من قابلية تطبيق نظام حماية البيانات الأوروبي على أنشطتها، وأثره عليها، إلى جانب اتخاذ التدابير المناسبة لضمان الامتثال للنظام، والحد من مخاطر مخالفته.

لمزيد من المعلومات حول ما ورد في هذه الوثيقة

يمكن التواصل على البريد الالكتروني

gdpr@nca.gov.sa

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority