سلسلة نظام حماية البيانات الشخصية في المملكة العربية السعودية

الجزء الثاني - ملخص اللائحة التنفيذية

pwc

مقدمة

سوف تدخل اللائحة التنفيذية حيز التنفيذ بشكل كامل في المملكة العربية السعودية ("**المملكة**") اعتبارًا من ١٤ سبتمبر ٢٠٢٤.

تقدم اللائحة التنفيذية مزيدًا من التفاصيل حول متطلبات نظام حماية البيانات الشخصية ("**النظام**").

في هذا الجزء الثاني من سلسلة نظام حماية البيانات الشخصية نقدم نظرة عامة على بعض المتطلبات الأساسية للائحة التنفيذية للنظام. حيث يرجى الرجوع إلى الجزء الأول من السلسلة للحصول على نظرة عامة حول النظام ومفاهيمه الأساسية.

المتطلبات الرئيسية للائحة التنفيذية

الحوكمة

- تلزم اللائحة التنفيذية جهة التحكم بتعيين مسؤول حماية البيانات في أي من الحالات التالية:
  - جهة التحكم هي الجهة العامة التي تقدم خدمات تتضمن معالجة البيانات الشخصية على نطاق واسع.
  - الأنشطة الأساسية لجهة التحكم تتكون من عمليات المعالجة التي تتطلب مراقبة منتظمة وممنهجة للأفراد.
  - الأنشطة الأساسية لجهة التحكم تتكون من معالجة البيانات الشخصية الحساسة.
- تحدد اللائحة التنفيذية المسؤوليات الرئيسية لمسؤول حماية البيانات على النحو التالي:
  - العمل كنقطة اتصال مباشرة مع الجهة المختصة وتنفيذ قراراتها وتعليماتها.
  - الإشراف على إجراءات تقويم الأثر التي يتعين إجراؤها، وتقارير التدقيق، والتقييمات، وتوثيق نتائج التقييم.
  - متابعة وتحديث سجلات أنشطة معالجة البيانات الشخصية.
  - تمكين أصحاب البيانات من ممارسة حقوقهم.
  - الرد على طلبات أصحاب البيانات ومعالجة شكواهم.
  - إخطار الجهة المختصة وأصحاب البيانات بخرق (تسرّب) البيانات حسب الاقتضاء.
  - التعامل مع مخالفات جهة التحكم المتعلقة بالبيانات الشخصية واتخاذ الإجراءات التصحيحية وفقًا لذلك.

وفقًا للفقرة رقم ٤ من المادة رقم ٣٢ من اللائحة التنفيذية، سوف تصدر الجهة المختصة قواعد تعيين مسؤول حماية البيانات والظروف التي ينبغي أن يتم بموجبها تعيين مسؤول حماية البيانات، وكذلك واجباته ومسؤولياته.

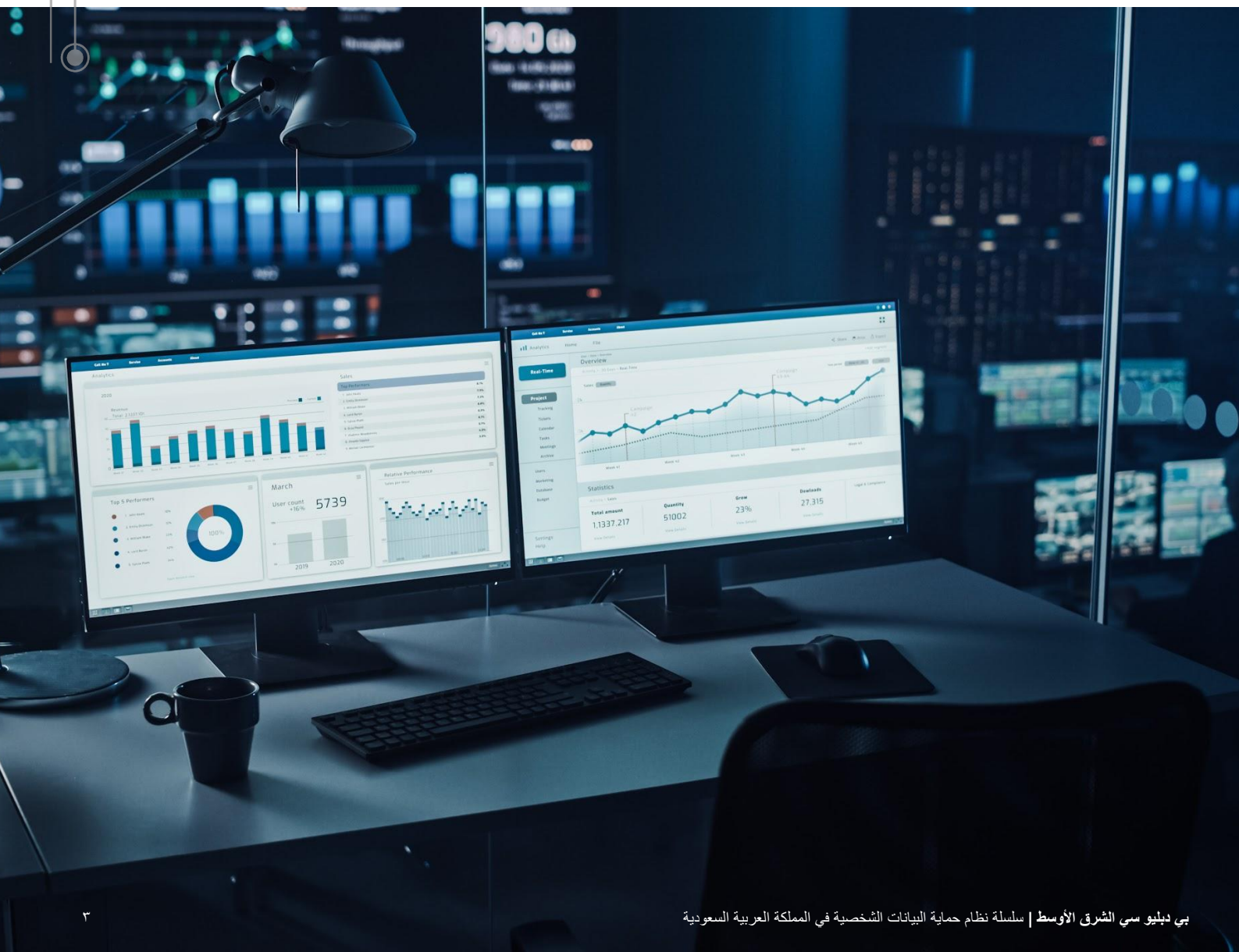
المادة رقم ٣٢ من النظام

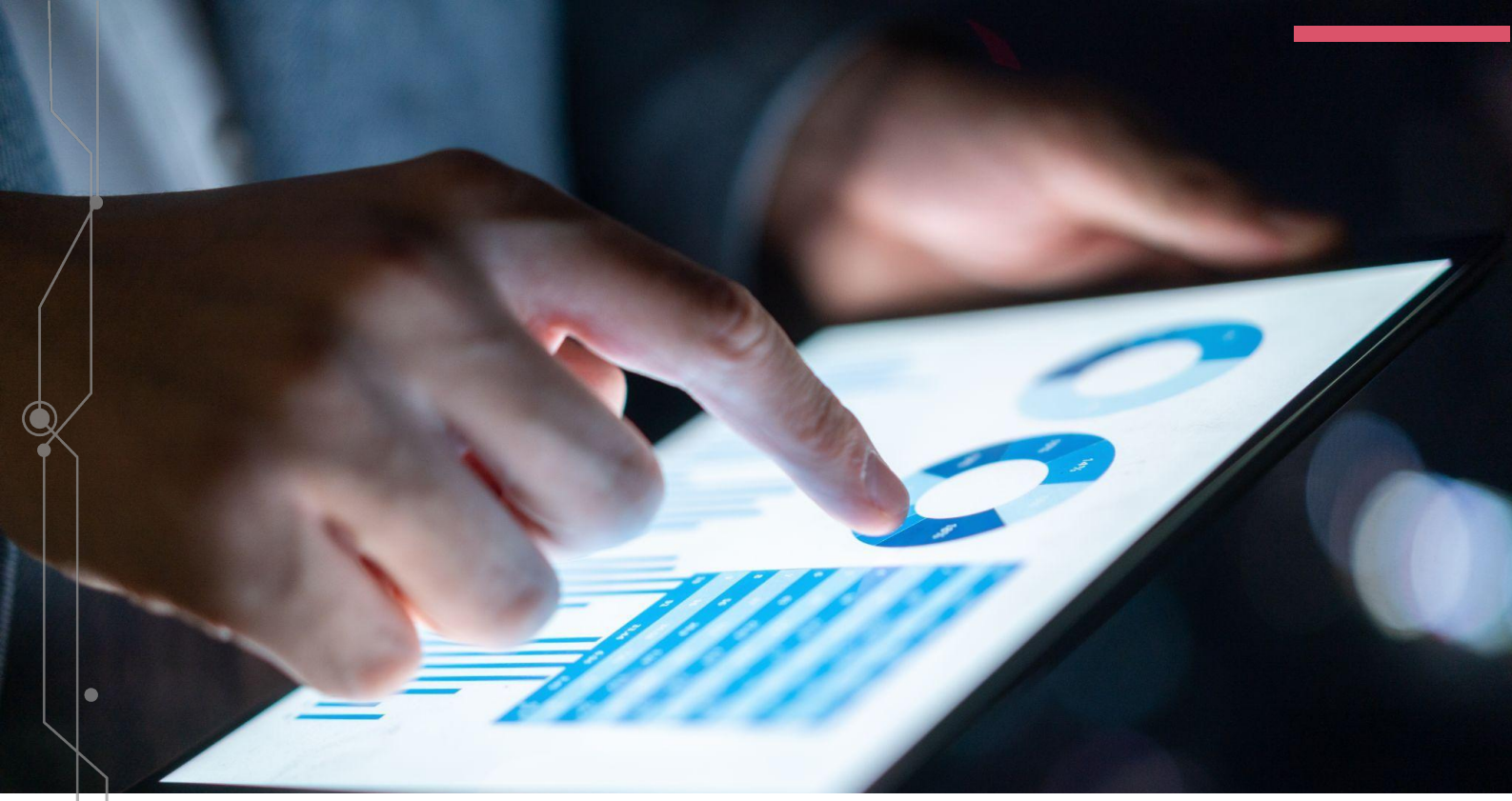
حقوق أصحاب البيانات الشخصية

تحدد اللائحة التنفيذية القواعد التي يتعين على جهة التحكم اتباعها عند تلقي طلب من صاحب البيانات. على سبيل المثال، ينبغي أن تقوم جهة التحكم بما يلي:

- الامتثال للطلب خلال مدة لا تتجاوز ٣٠ يومًا، والتي يمكن تمديدها حتى ٣٠ يومًا إضافية في حالة تَطلَّب الرد جهدًا إضافيًا غير متوقع أو غير معتاد، أو إذا تلقت جهة التحكم طلبات متعددة من صاحب البيانات.
- اتخاذ التدابير الفنية والإدارية والتنظيمية اللازمة لضمان الرد السريع على الطلبات.
- اتخاذ الإجراءات المناسبة للتحقق من هوية مقدم الطلب قبل تنفيذ الطلب.
- اتخاذ الإجراءات اللازمة لتوثيق وتسجيل جميع الطلبات المقدمة، بما في ذلك الطلبات الشفهية.
- يمكن لجهة التحكم رفض التصرف بناءً على الطلب عندما يكون متكررًا بشكل غير مبرر أو يتطلب جهودًا غير متناسبة.

المادة رقم ٣ من النظام





تنص اللائحة التنفيذية على تفاصيل إضافية حول الكيفية التي تضمن بها جهة التحكم أن أصحاب البيانات يمكنهم ممارسة حقوقهم وعلى سبيل المثال:

- الحق في العلم (بما في ذلك المعلومات التي ينبغي تقديمها إلى صاحب البيانات وكيفية ذلك).
- الحق في الوصول إلى البيانات (بما في ذلك الضمانات اللازمة لحماية البيانات الشخصية عند الإفصاح عنها).
- الحق في التصحيح (بما في ذلك حق صاحب البيانات في طلب تقييد معالجة البيانات الشخصية خلال التحقق من صحة البيانات الشخصية، وما إلى ذلك).
- الحق في إتلاف البيانات (بما في ذلك أسباب وكيفية القيام بهذا الإتلاف).

من المادة رقم ٤ إلى المادة رقم ٨ من النظام

تنص اللائحة على تفاصيل حول كيفية قيام صاحب البيانات بتقديم شكوى إلى الجهة المختصة، على سبيل المثال:

- المدة الزمنية التي يمكن خلالها تقديم الشكوى (خلال مدة لا تتجاوز ٩٠ يومًا من تاريخ الحادث أو التاريخ الذي أصبح فيه صاحب البيانات على علم به).
- محتويات الشكوى.
- الإجراءات الرئيسية التي تتخذها الجهة المختصة فيما يتعلق بالشكوى.

المادة رقم ٣٧ من النظام

الموافقة

- تحدد اللائحة التنفيذية شروط الموافقة كمسوغ نظامي لمعالجة البيانات الشخصية:

- أن تصدر الموافقة بإرادة حرة ولا يتم الحصول عليها بطرق مضللة.

- أن تكون أغراض المعالجة واضحة ومحددة ويجب شرحها وتوضيحها لصاحب البيانات الشخصية قبل أو أثناء وقت طلب الموافقة.

- أن تصدر الموافقة من فرد يتمتع بكامل الأهلية.

- يتعين توثيق الموافقة.

- الحصول على موافقة مستقلة لكل غرض من أغراض المعالجة.

- تضع جهة التحكم الإجراءات التي تسمح بالعدول عن تلك الموافقة، قبل طلب الموافقة من صاحب البيانات.

- في حالة العدول عن الموافقة، تتوقف جهة التحكم عن المعالجة دون تأخير غير مبرر بعد طلب العدول.

- تنص اللائحة التنفيذية على أن الموافقة صريحة في بعض الحالات، على سبيل المثال:

- تتضمن المعالجة بيانات حساسة.

- تتضمن المعالجة بيانات ائتمانية.

- لا يتم اتخاذ القرارات إلا على أساس المعالجة الآلية للبيانات الشخصية.

الموافقة الصريحة تعني الموافقة المباشرة والصريحة التي يمنحها صاحب البيانات بأي شكل من الأشكال والتي تشير بوضوح إلى قبول صاحب البيانات لمعالجة بياناته الشخصية بطريقة لا يمكن تفسيرها بشكل آخر، والتي يمكن إثبات نيتها. في الأساس، ينبغي أن يكون هناك إجراء إيجابي يتعين على صاحب البيانات اتخاذه إقرارًا بالموافقة (على سبيل المثال: النقر فوق مربع الموافقة غير المحدد).

المادة رقم ١١ والمادة رقم ١٢ من النظام

المصلحة المشروعة

- تحدد اللائحة التنفيذية متطلبات استخدام المصلحة المشروعة كمسوغ نظامي. على سبيل المثال، من الممكن استخدام المصلحة المشروعة إذا استوفيت الشروط التالية:

  - ألا يكون الغرض مخالفًا لأي من الأنظمة في المملكة.
  - أن يكون هناك توازن بين حقوق ومصالح صاحب البيانات الشخصية والمصلحة المشروعة لجهة التحكم، بحيث لا تؤثر مصالح جهة التحكم على حقوق ومصالح صاحب البيانات.
  - ألا تشمل المعالجة بيانات حساسة.
  - أن تكون المعالجة ضمن التوقعات المعقولة لصاحب البيانات الشخصية.

- تقوم جهة التحكم قبل معالجة البيانات الشخصية للمصلحة المشروعة بإجراء وتوثيق تقييم للمعالجة المقترحة وأثرها على حقوق ومصالح أصحاب البيانات والتي يتعين أن تشمل:

  - تحديد المعالجة المقترحة وأغراضها، وكذلك نوع البيانات وفئات أصحاب البيانات الشخصية.
  - تقييم الغرض للتأكد من شرعيته ومطابقته لأنظمة المملكة.
  - التحقق من ضرورة معالجة البيانات الشخصية لتحقيق الغرض المشروع لجهة التحكم.
  - تقييم ما إذا كانت المعالجة المقترحة ستسبب أي ضرر محتمل لأصحاب البيانات الشخصية أو قدرتهم على ممارسة حقوقهم.
  - تحديد أي إجراءات يتعين اتخاذها لتجنب المخاطر أو الأضرار المحتملة.

المادة رقم ١٦

تقويم الأثر

- تحدد اللائحة التنفيذية الحالات التي يتعين فيها على جهة التحكم إجراء تقويم أثر حماية البيانات، على وجه الخصوص عندما:

- تتضمن المعالجة معالجة بيانات الحساسة.

- تقوم جهة التحكم بجمع أو مقارنة أو ربط مجموعتين أو أكثر من البيانات الشخصية التي تم الحصول عليها من مصادر مختلفة.

- يشمل نشاط جهة التحكم المعالجة المستمرة والواسعة النطاق للبيانات الشخصية لأولئك الذين يفتقرون كليًا أو جزئيًا إلى الأهلية القانونية، أو معالجة العمليات التي تتطلب بطبيعتها مراقبة مستمرة لأصحاب البيانات، أو معالجة البيانات الشخصية باستخدام تقنيات جديدة، أو اتخاذ قرارات تستند إلى المعالجة الآلية للبيانات الشخصية.

- توفر جهة التحكم منتجًا أو خدمة تتضمن معالجة البيانات الشخصية التي من المحتمل أن تسبب ضررًا جسيمًا لخصوصية أصحاب البيانات الشخصية.

- تحدد اللائحة التنفيذية متطلبات لمحتوى تقويم أثر حماية البيانات والتي ينبغي أن تتضمن المعلومات التالية (التي سيتم تحديدها في تقرير تقويم أثر حماية البيانات):

- الغرض من المعالجة ومسوغاتها النظامية.

- وصف لطبيعة المعالجة و أنواع ومصادر البيانات الشخصية والجهات التي تفصح لها بالبيانات الشخصية.

- وصف لنطاق المعالجة.

- وصف سياق المعالجة.

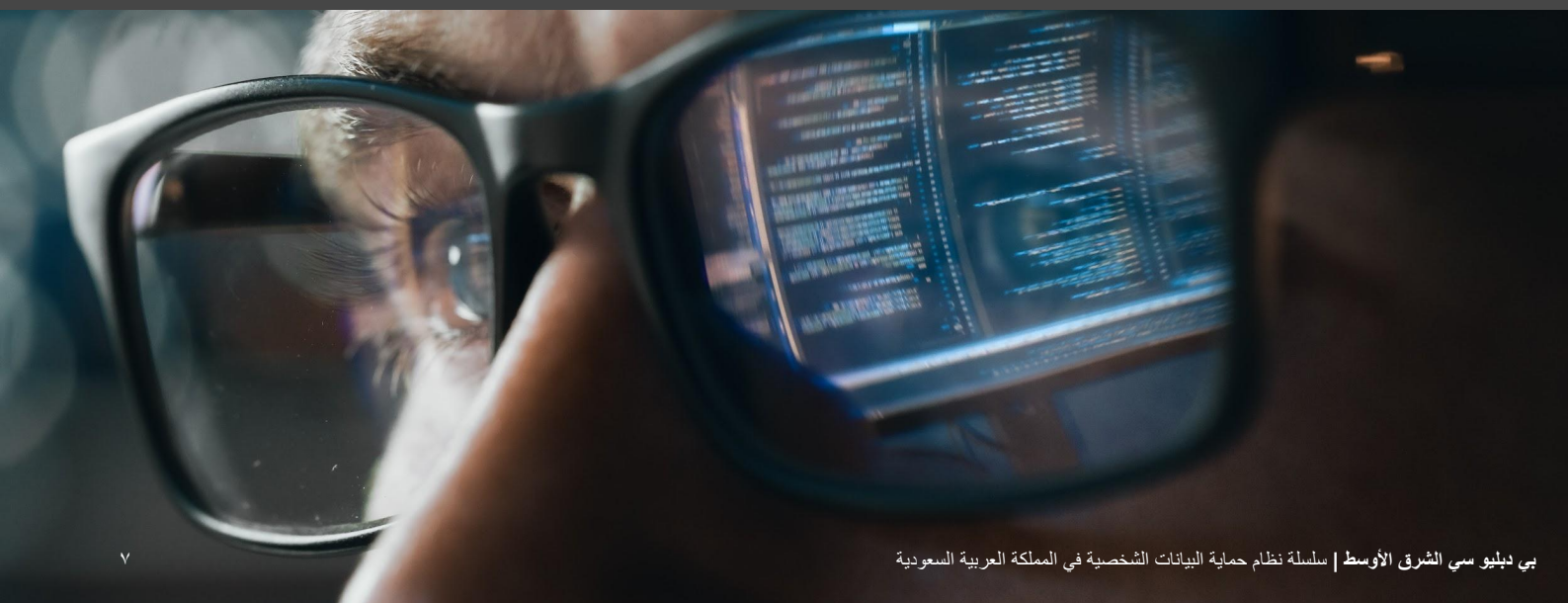
- تقييم مدى ضرورة وتناسب التدابير التي يتعين اتخاذها.

- أثر المعالجة بناءً على مدى خطورة تأثيرها ماديًا ومعنويًا، واحتمال حدوث أي تأثير سلبي على أصحاب البيانات الشخصية.

- التدابير التي سيتم اتخاذها لمنع المخاطر أو الحد منها.

- تقييم مدى ملاءمة التدابير المتخذة لتجنب المخاطر المحددة.

المادة رقم ٢٥ من النظام



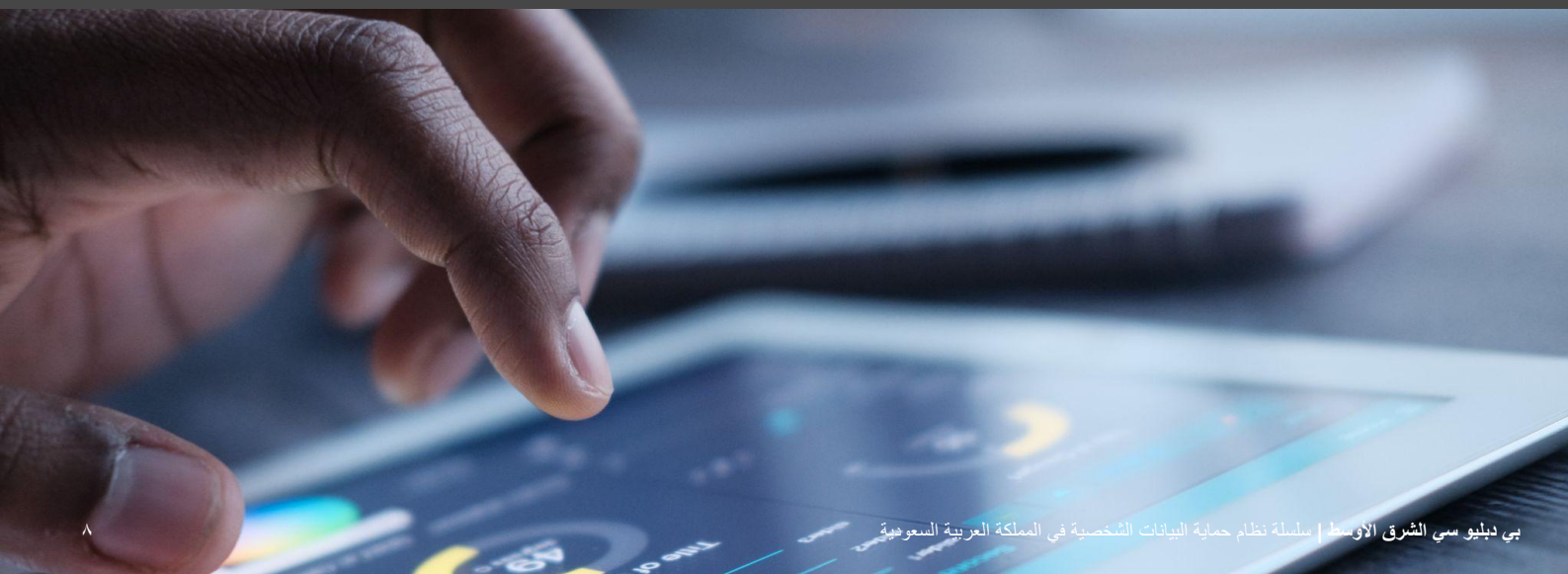
سجلات أنشطة معالجة البيانات الشخصية

- تحدد اللائحة التنفيذية شروط الاحتفاظ بسجلات أنشطة معالجة البيانات الشخصية. تتضمن هذه السجلات المعلومات التالية:
  - اسم جهة التحكم ومعلومات الاتصال ذات الصلة.
  - معلومات حول مسؤول حماية البيانات، إذا كان تعيين مسؤول حماية البيانات مطلوبًا وفقًا للمادة رقم ٣٢ من اللائحة التنفيذية.
  - أغراض معالجة البيانات الشخصية.
  - وصف فئات البيانات الشخصية التي تجري معالجتها.
  - فئات أصحاب البيانات.
  - فترات الاحتفاظ لكل فئة من البيانات الشخصية.
  - فئات الجهات التي يتم الإفصاح لها عن البيانات الشخصية.
  - وصف عمليات نقل البيانات الشخصية خارج المملكة بما في ذلك المسوغات النظامية لعمليات نقل البيانات الشخصية والجهات التي يتم نقل البيانات الشخصية إليها.
  - وصف الإجراءات والتدابير التنظيمية والإدارية والفنية المعمول بها والتي تكفل أمن البيانات الشخصية.

المادة رقم ٣٣ من النظام

- تنص اللائحة التنفيذية على اشتراطات لأنواع معينة من أنشطة معالجة البيانات الشخصية، على سبيل المثال:
  - معالجة البيانات الصحية.
  - معالجة بيانات الائتمان.
  - معالجة البيانات لأغراض الإعلان أو التوعية.
  - معالجة البيانات للتسويق المباشر.
  - معالجة البيانات للأغراض العلمية أو البحثية أو الإحصائية.

من المادة رقم ٢٦ إلى المادة رقم ٣٠ من النظام



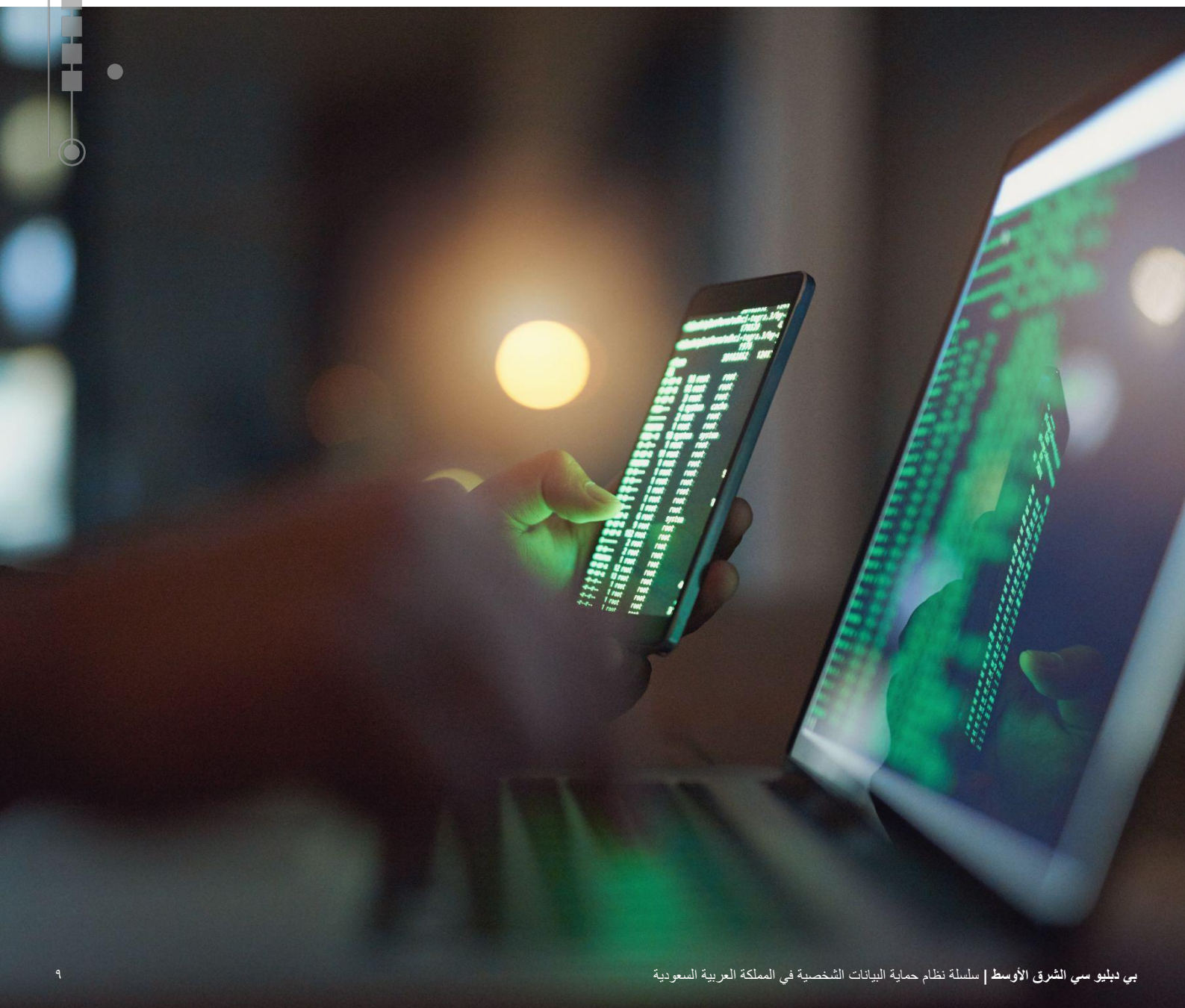
إدارة خرق[1] البيانات

تنص اللائحة التنفيذية على تفاصيل بشأن التزام جهة التحكم بإخطار الجهة المختصة وأصحاب البيانات الشخصية بخرق البيانات الشخصية:

- تقدم جهة التحكم إخطارًا إلى الجهة المختصة خلال ٧٢ ساعة من علمه بالحادثة، إذا كان من المحتمل أن تتسبب هذه الحادثة في إلحاق ضرر بالبيانات الشخصية، أو لأصحاب البيانات أو تتعارض مع حقوقهم أو مصالحهم.
- تقوم جهة التحكم، دون تأخير، بإخطار أصحاب البيانات إذا كان الخرق قد يسبب ضررًا لبياناتهم أو يتعارض مع حقوقهم أو مصالحهم.
- تحدد اللائحة التنفيذية متطلبات محتوى الإخطار بالخرق الواجب تقديمه إلى الجهة المختصة أو أصحاب البيانات.

المادة رقم ٢٤

[1] تم استخدام مصطلح "تسرب البيانات الشخصية" في اللائحة.



التعامل مع جهة المعالجة

تحدد اللائحة التنفيذية المتطلبات الأساسية للتعاون بين جهة التحكم وجهة المعالجة، وعلى وجه الخصوص:

- يجب أن تتضمن الشروط والأحكام التي ينبغي إدراجها في اتفاقية معالجة البيانات بين جهة التحكم وجهة المعالجة، على الأقل، ما يلي:
  - غرض المعالجة.
  - فئات البيانات الشخصية التي تتم معالجتها.
  - المدة الزمنية للمعالجة.
  - التزام جهة المعالجة بإخطار جهة التحكم بخرق البيانات الشخصية.
  - توضيح ما إذا كانت جهة المعالجة تخضع لأنظمة في دول أخرى، وأثر ذلك على التزامها بأحكام النظام ولوائحه.
  - التزام جهة المعالجة بإخطار جهة التحكم بالإفصاح عن البيانات الشخصية والذي قد يكون إلزاميًا بموجب الأنظمة السارية في المملكة.
  - تحديد أي جهات أخرى تتعاقد معهم جهة المعالجة، أو أي طرف آخر يتم الإفصاح له عن البيانات الشخصية.
- تصدر جهة التحكم تعليمات واضحة إلى جهة المعالجة.
- تقوم جهة التحكم بالتحقق من التزام جهة المعالجة بنظام حماية البيانات الشخصية واللوائح.
- تلتزم جهة المعالجة بمتطلبات معينة عند إبرام اتفاقيات مع جهة المعالجة الفرعية.

المادة رقم ١٧ من النظام

أمن المعلومات

تنص اللائحة التنفيذية على تفاصيل عن التدابير التي يتعين على جهة التحكم اتخاذها لضمان أمن البيانات الشخصية. على سبيل المثال، تتطلب اللائحة التنفيذية من جهة التحكم ما يلي:

- تنفيذ التدابير الأمنية والفنية اللازمة للحد من المخاطر الأمنية المتعلقة بخرق البيانات الشخصية.
- الالتزام بالضوابط والمعايير والقواعد ذات الصلة الصادرة عن الهيئة الوطنية للأمن السيبراني في المملكة أو أفضل الممارسات ومعايير الأمن السيبراني المعترف بها إذا لم تكن جهة التحكم ملزمة باتباع الضوابط والمعايير والقواعد الصادرة عن الهيئة الوطنية للأمن السيبراني في المملكة.

المادة رقم ٢٣ من النظام

التواصل معنا

يُرجى التواصل معنا لمناقشة كيف يمكن لشركة بي دبليو سي الشرق الأوسط المساعدة في تنفيذ برنامج حماية البيانات الشخصية لديكم.

فيل ميني
مدير تنفيذي في فريق الثقة الرقمية والأمن السيبراني
+971 56 369 7736
phil.mennie@pwc.com
linkedin.com/in/philmennie
@philmennie

ريتشارد تشودزينسكي
مدير الفريق القانوني في فريق الثقة الرقمية والأمن السيبراني
+971 56 417 6591
richard.chudzynski@pwc.com
linkedin.com/in/richardchudzynski

شكراً لكم