سلسلة نظام حماية البيانات الشخصية في المملكة العربية السعودية

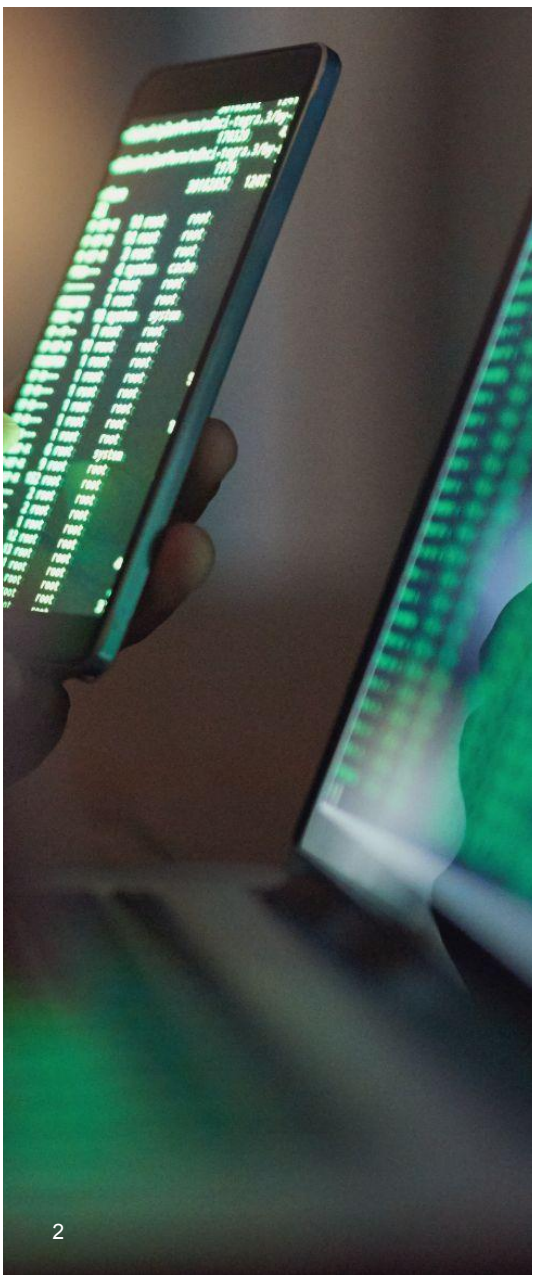
الجزء الأول – ملخص نظام حماية البيانات الشخصية

pwc

مقدمة

يتناول الدليل حول نظام حماية البيانات الشخصية في المملكة العربية السعودية الجوانب الثلاثة التالية:

1. الجزء الأول: ملخص نظام حماية البيانات الشخصية (**"النظام" أو "القانون"**).
2. الجزء الثاني: ملخص اللائحة التنفيذية لنظام حماية البيانات الشخصية (**"اللائحة التنفيذية"**).
3. الجزء الثالث: الدليل حول نقل البيانات الشخصية خارج المملكة العربية السعودية بناءً على لائحة نقل البيانات الشخصية خارج المملكة (**"لائحة نقل البيانات"**)[١].



دخل نظام حماية البيانات الشخصية حيز التنفيذ في المملكة العربية السعودية (**"المملكة"**) في ١٤ سبتمبر ٢٠٢٣. وهو النظام (أو القانون) الرئيسي في المملكة الذي ينظم استخدام البيانات الشخصية. اعتبارًا من ١٤ سبتمبر ٢٠٢٣ سيكون أمام الجهات الخاضعة لنظام حماية البيانات الشخصية واللوائح **عام واحد للامتثال لها**. وسوف يدخل النظام واللوائح حيز التنفيذ بشكل كامل اعتبارًا من ١٤ سبتمبر ٢٠٢٤.

يجب على **جميع الجهات العامة والخاصة** الالتزام بنظام حماية البيانات الشخصية واللوائح.

الهيئة السعودية للبيانات والذكاء الاصطناعي ("**سدايا**"**)** هي الجهة المختصة التي تشرف على تنفيذ النظام واللوائح. ويجوز للجهة المختصة أن تطلب مستندات أو معلومات من الجهات للتحقق من مدى امتثالها للنظام واللوائح.

ينص نظام حماية البيانات الشخصية على **غرامات (تصل إلى ٥,٠٠٠,٠٠٠ ريالًا سعوديًا)** لمخالفة أحكامه وأحكام اللوائح. ويجوز للمحكمة المختصة مضاعفة مبلغ الغرامة في حالة تكرار المخالفات. وينص النظام أيضًا على السجن (لمدة تصل إلى عامين) في حالة الإفصاح عن بيانات حساسة أو نشرها (بشكل ينتهك النظام) بقصد إيذاء فرد أو تحقيق مكاسب شخصية.

في هذا الجزء الأول من سلسلتنا، نلقي نظرة على المفاهيم الأساسية لنظام حماية البيانات الشخصية وما تعنيه هذه المفاهيم بالنسبة للجهات التي تمارس الأعمال التجارية في المملكة.

[١] في هذه السلسلة نشير بشكل مشترك إلى اللائحة التنفيذية ولائحة نقل البيانات بمصطلح موحد "اللوائح".

نطاق النظام

أ ـ ما الذي ينظمه نظام حماية البيانات الشخصية؟

ينظم القانون معالجة[٢] البيانات الشخصية ويشمل نطاقه ما يلي:

١	٢	٣
معالجة البيانات الشخصية من أي نوع ـ على سبيل المثال: معلومات الاتصال، والبيانات الصحية، والبيانات الائتمانية، وما إلى ذلك.	معالجة البيانات الشخصية من أي مصدر ـ على سبيل المثال: البيانات المقدمة من الأفراد مباشرة إلى الجهات أو التي تحصل عليها الجهة من مصادر أخرى، وما إلى ذلك.	معالجة البيانات الشخصية بأي شكل من الأشكال ـ على سبيل المثال: إلكترونية أو ورقية، المهيكلة أو غير المهيكلة، وما إلى ذلك.

بيانات شخصية

تعرف البيانات الشخصية في النظام على النحو التالي[٣]: كل بيان ـ مهما كان مصدره أو شكله ـ من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكنًا بصفة مباشرة أو غير مباشرة، ومن ضمن ذلك: الاسم، ورقم الهوية الشخصية، والعناوين، وأرقام التواصل، وأرقام الرخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي. ولذلك، فإن أي بيانات يمكن من خلالها تحديد هوية فرد ما سيتم اعتبارها بيانات شخصية بموجب النظام. **أمثلة:**

اسم الفرد	رقم الهاتف	رقم الحساب البنكي

إذا كان من المستحيل تحديد فرد معين من البيانات المعنية، فإن هذه البيانات ليست بيانات شخصية ولا ينظم النظام استخدامها ـ على سبيل المثال، البيانات التي خضعت لإخفاء الهوية، وأرقام المبيعات، والبيانات المتعلقة بعدد الزيارات الإجمالية لصفحة الويب.

البيانات الحساسة

يوفر النظام مجموعة فرعية منفصلة من البيانات الشخصية وهي البيانات الحساسة. وتشمل البيانات الحساسة كل بيان شخصي يتعلق بأصل الفرد العرقي أو أصله الإثني، أو معتقده الديني أو الفكري أو السياسي. وكذلك البيانات الأمنية والجنائية، أو بيانات السمات الحيوية التي تحدد الهوية، أو البيانات الوراثية، أو البيانات الصحية، والبيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهما.

ينص النظام على متطلبات وقيود إضافية لمعالجة البيانات الحساسة. على سبيل المثال:

- يحظر الاعتماد على مسوغ نظامي "المصالح المشروعة" عند معالجة البيانات الحساسة[٤].
- يحظر استخدام البيانات الحساسة لأغراض تسويقية[٥].

يرجى ملاحظة أنه على عكس العديد من قوانين حماية البيانات الأخرى، ينظم النظام أيضًا معالجة بيانات الأشخاص المتوفين إذا كانت هذه البيانات تسمح بتحديد هوية الشخص المتوفى أو أفراد أسرته.

٢ المعالجة تعني أي طريقة من استخدام البيانات الشخصية.
٣ الفقرة رقم ٤ من المادة رقم ١ من النظام.
٤ الفقرة رقم ٤ من المادة رقم ٦ من النظام.
٥ المادة رقم ٢٦ من النظام.

ب - نطاق تطبيق النظام

ينطبق النظام على عمليات المعالجة التالية للبيانات الشخصية بأي وسيلة (يدوية أو آلية):

داخل المملكة العربية السعودية

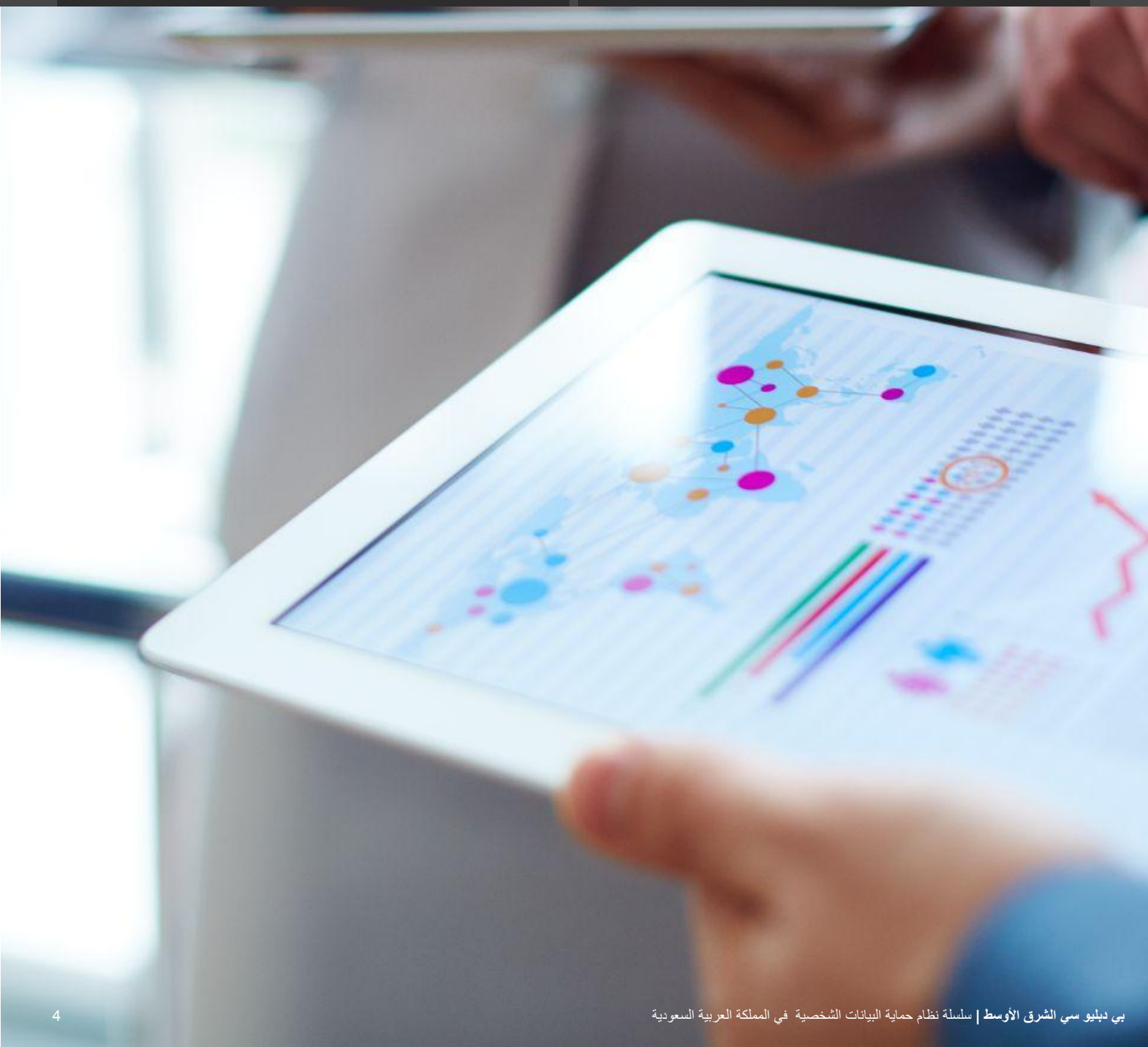
ينظم القانون أي معالجة للبيانات الشخصية تتم في المملكة، مما يعني أن النظام ينطبق على معالجة البيانات الشخصية في جميع المناطق التي تتمتع المملكة بسلطتها، بما في ذلك الإقليم الجغرافي للمملكة وسفاراتها في الولايات القضائية الأجنبية.

١

خارج المملكة العربية السعودية

ينظم القانون أي معالجة للبيانات الشخصية للمقيمين في المملكة والتي يتم القيام بها من قبل أي جهة خارج المملكة، مما يعني أن النظام يمكن أن يطبَّق خارج الحدود الإقليمية فيما يتعلق بالمقيمين في المملكة. وقد يشمل ذلك المواطنين السعوديين وغيرهم من الأفراد الذين يقيمون في المملكة بشكل دائم أو مؤقت.

٢



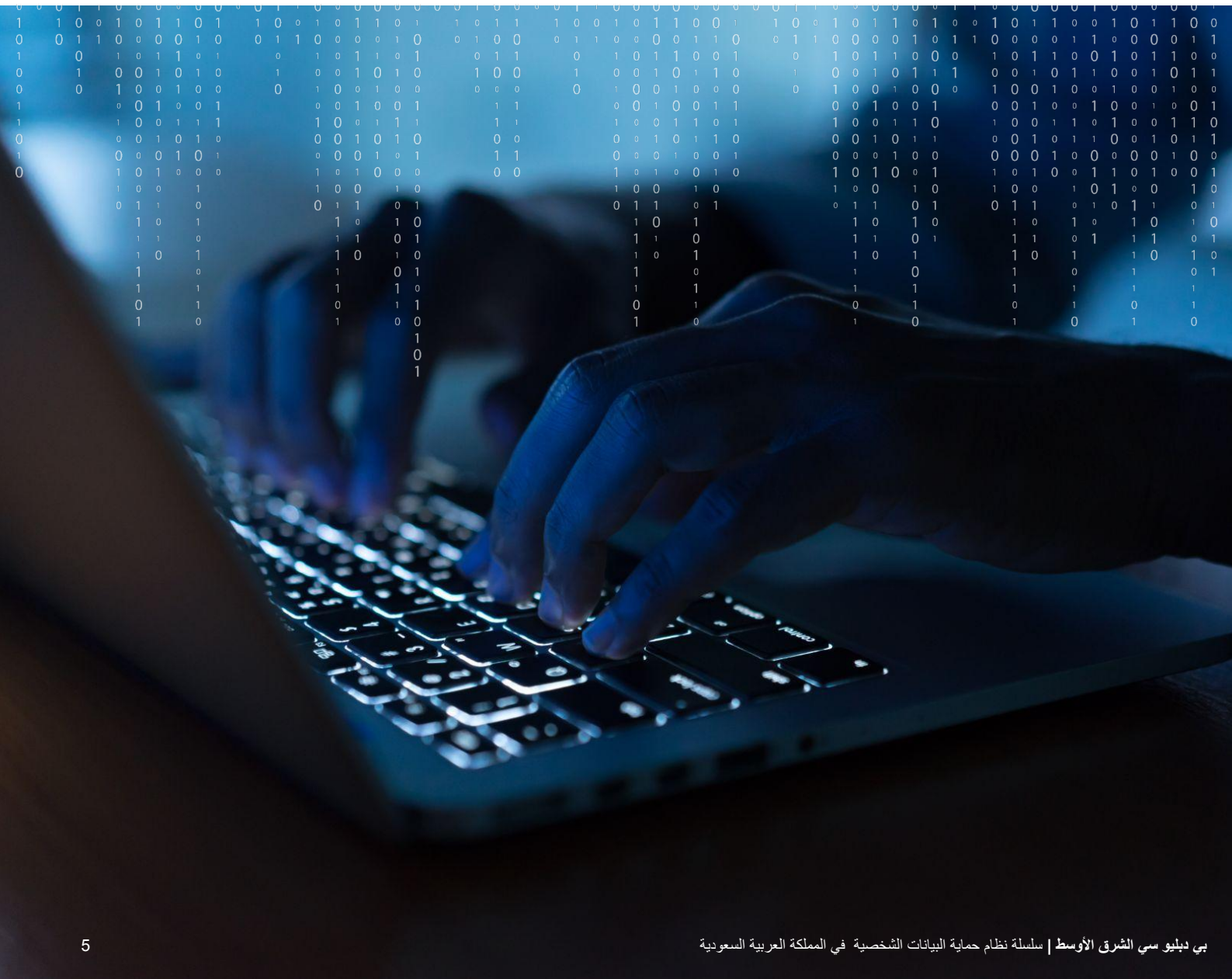
أدوار الجهة والتزاماتها بموجب النظام

أ - ما هي الأدوار التي يمكن للجهات أن تتولاها بموجب النظام؟

ينص النظام على دورين للجهات فيما يتعلق بمعالجة البيانات الشخصية ألا وهما، جهة التحكم وجهة المعالجة.

جهة التحكم هي من تتخذ القرارات بشأن أغراض وطرق معالجة البيانات الشخصية. حيث تتحمل جهة التحكم في النهاية المسؤولية عن المعالجة بموجب النظام.

جهة المعالجة هي من تقوم بمعالجة البيانات الشخصية نيابة عن جهة التحكم. على عكس جهة التحكم، لا تتخذ جهة المعالجة قرارات بشأن أغراض وطرق معالجة البيانات الشخصية وبدلًا من ذلك تأخذ التوجيهات من جهة التحكم.



ب - ما هي الالتزامات الأساسية لجهة التحكم؟

- تحديد الغرض من معالجة البيانات الشخصية.
- التأكد من وجود مسوغ نظامي مناسب لمعالجة البيانات الشخصية (على سبيل المثال: الموافقة، والالتزام النظامي، والمصالح المشروعة، وما إلى ذلك).
- ضمان معالجة البيانات الشخصية وفقًا لمبادئ معالجة البيانات الشخصية (على سبيل المثال: محدودية التخزين - يرجى الاطلاع على مبادئ معالجة البيانات الشخصية).
- إخطار أصحاب البيانات[٦] حول كيفية معالجة بياناتهم الشخصية (على سبيل المثال: عبر إشعار الخصوصية).
- تمكين أصحاب البيانات من ممارسة حقوقهم بموجب النظام.
- الاحتفاظ بسجلات أنشطة المعالجة لجميع عمليات معالجة البيانات الشخصية عبر الجهة.
- إجراء تقويم الأثر في معالجة البيانات الشخصية (على سبيل المثال: تقويم الأثر حول حماية البيانات أو تقويم الأثر حول نقل البيانات أو حول المصالح المشروعة).
- ضمان نقل البيانات الشخصية عبر الحدود الجغرافية للمملكة بطريقة نظامية.
- تنفيذ كافة الإجراءات التنظيمية والإدارية والفنية اللازمة لحماية البيانات الشخصية.
- التعاون فقط مع جهات المعالجة التي تقدم الضمانات اللازمة لتنفيذ أحكام النظام واللوائح، وإبرام اتفاقيات معالجة البيانات مع جهات المعالجة، ومراقبة امتثال جهات المعالجة لهذه الاتفاقيات.
- إخطار الجهات التي تم نقل البيانات الشخصية إليها بأي تغييرات في البيانات الشخصية.
- إخطار الجهة المختصة وأصحاب البيانات بخرق البيانات الشخصية.
- تعيين مسؤول حماية البيانات، حيثما تقتضي اللائحة التنفيذية ذلك[٧].
- الامتثال لمتطلبات النظام واللائحة لأنواع محددة من أنشطة المعالجة، على سبيل المثال:

- معالجة البيانات الصحية وبيانات الائتمان.
- معالجة البيانات الشخصية لإرسال مواد إعلانية أو توعوية.
- معالجة البيانات الشخصية للأغراض العلمية أو البحثية أو الإحصائية.
- الإفصاح عن البيانات الشخصية.
- نسخ المستندات الرسمية حيث يمكن تعريف أصحاب البيانات.

- الامتثال لقواعد تسجيل جهة التحكم في السجِّل الوطني لجهات التحكم (سوف تصدرها الجهة المختصة).

---

٦ أصحاب البيانات هم الأفراد الذين تتم معالجة بياناتهم الشخصية.
٧ الفقرة رقم ٢ من المادة رقم ٣٠ من النظام.

ج - ما هي الالتزامات الأساسية لجهة المعالجة؟

• معالجة البيانات الشخصية لجهة التحكم وفقًا لاتفاقية معالجة البيانات.

• الالتزام بتعليمات جهة التحكم فيما يتعلق بمعالجة البيانات الشخصية.

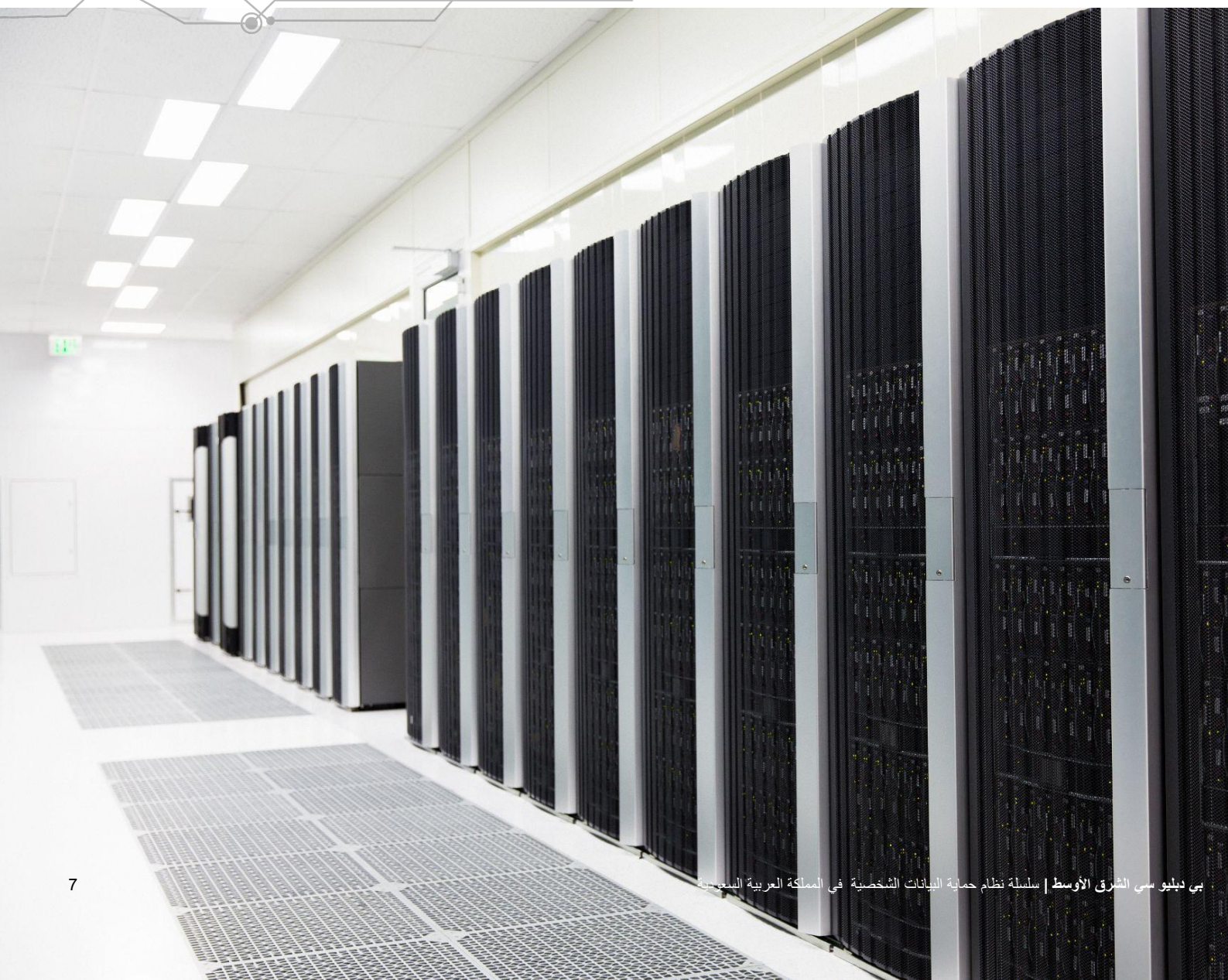
• مساعدة جهة التحكم من خلال تنفيذ الإجراءات التنظيمية والإدارية والفنية المناسبة لحماية البيانات الشخصية التي تتم معالجتها لجهة التحكم.

• قبل أن تتعامل جهة المعالجة مع أي جهة للمعالجة الفرعية، يجب ضمان ما يلي:

- لن تؤثر العقود المبرمة مع جهات المعالجة الفرعية على مستوى الحماية المقدمة للبيانات الشخصية التي تتم معالجتها.

- توفر جهات المعالجة الفرعية ضمانات كافية للامتثال للنظام واللوائح.

-يجب على جهة المعالجة إخطار جهة التحكم بشأن إشراك جهة المعالجة الفرعية وتكون لجهة التحكم الحق في الاعتراض على هذه المشاركة خلال مدة يتفق عليها كلًا من جهة التحكم وجهة المعالجة.



مبادئ معالجة البيانات الشخصية

على الرغم من أن النظام لا يذكر صراحةً أي مبادئ حول حماية البيانات الشخصية، إلا أن هذه المبادئ مضمنة في أحكام النظام. كما يساعد فهم هذه المبادئ على فهم متطلبات النظام.

المبدأ	وصف المبدأ
النظامية والأمانة والشفافية	●يجب التأكد من جمع البيانات الشخصية استنادًا إلى مسوغ نظامي. ●يلزم معالجة البيانات الشخصية في جميع الأوقات بما يتوافق مع الأنظمة واللوائح المعمول بها في المملكة. ●ينبغي تزويد الأفراد بما يوضح لهم كيفية معالجة بياناتهم الشخصية.
محدودية الغرض	●يجب أن يكون لدى الجهة غرض محدد لمعالجة البيانات الشخصية. ●يجب كذلك تحديد الغرض من جمع البيانات الشخصية وتوثيقه في سجل أنشطة المعالجة.
تقليل البيانات	ينبغي الامتناع عن جمع بيانات شخصية بطريقة تزيد على الحاجة من أجل تحقيق الغرض من المعالجة، لذا إذا لم تكن هنالك حاجة إلى البيانات الشخصية، يجب الامتناع عن جمعها.
محدودية التخزين	ينبغي الامتناع عن تخزين البيانات الشخصية لفترة أطول من الفترة المناسبة لتحقيق أغراض معالجة البيانات الشخصية أو الفترة المحددة في الأنظمة واللوائح المعمول بها.
الدقة	يجب على الجهات: ●مراجعة البيانات الشخصية بطريقة مستمرة للتأكد من أنها صحيحة وكاملة ومحدثة. ●منح فرصة للأفراد لمراجعة بياناتهم الشخصية وتحديثها، إذا كانت هناك حاجة إلى ذلك.
النزاهة والسريّة	يجب اتخاذ إجراءات تنظيمية وإدارية وتقنية كافية من أجل حماية البيانات الشخصية وضمان سريّتها وسلامتها وإمكانية الوصول إليها أثناء نقلها وتخزينها.
المسؤولية	يجب اتخاذ إجراءات مناسبة وتوفير السجلات اللازمة لإثبات الالتزام بالأنظمة واللوائح والمبادئ المتعلقة بحماية البيانات الشخصية.

المسوغات النظامية لمعالجة البيانات الشخصية

يجب على جهة التحكم ضمان أنها تعالج البيانات الشخصية فقط إذا كان لديها مسوغ نظامي مناسب لهذه المعالجة. حيث ينص النظام على عدة مجموعات من المسوغات النظامية التي ينبغي استخدامها وفقًا لظروف المعالجة المحددة.

المسوغات النظامية العامة
(المادة رقم ٥ والمادة رقم ٦ من النظام)

- **الموافقة** - تم تقديم الموافقة من صاحب البيانات على معالجة بياناته الشخصية.
- **المصلحة المتحققة** - تتم المعالجة لمصلحة متحققة لفرد وكان الاتصال به صعبًا أو مستحيلًا.
- **الاتفاق** - تكون المعالجة ضرورية لتنفيذ الاتفاق السابق يكون صاحب البيانات الشخصية طرفًا فيه.
- **الالتزام النظامي** - تكون المعالجة ضرورية للالتزام بنظام آخر.
- **المصلحة العامة** - إذا كانت جهة التحكم جهة عامة، وكانت تلك المعالجة مطلوبة لأغراض أمنية أو لاستيفاء متطلبات قضائية.
- **المصالح المشروعة** - تكون معالجة البيانات الشخصية ضرورية لتحقيق مصالح مشروعة لجهة التحكم والتي لا تشمل البيانات الحساسة.

المسوغات النظامية (١) لجمع البيانات الشخصية من غير صاحبها مباشرةً و(٢) لمعالجتها لغرض آخر غير الذي جمعت من أجله
(المادة رقم ١٠ من النظام)

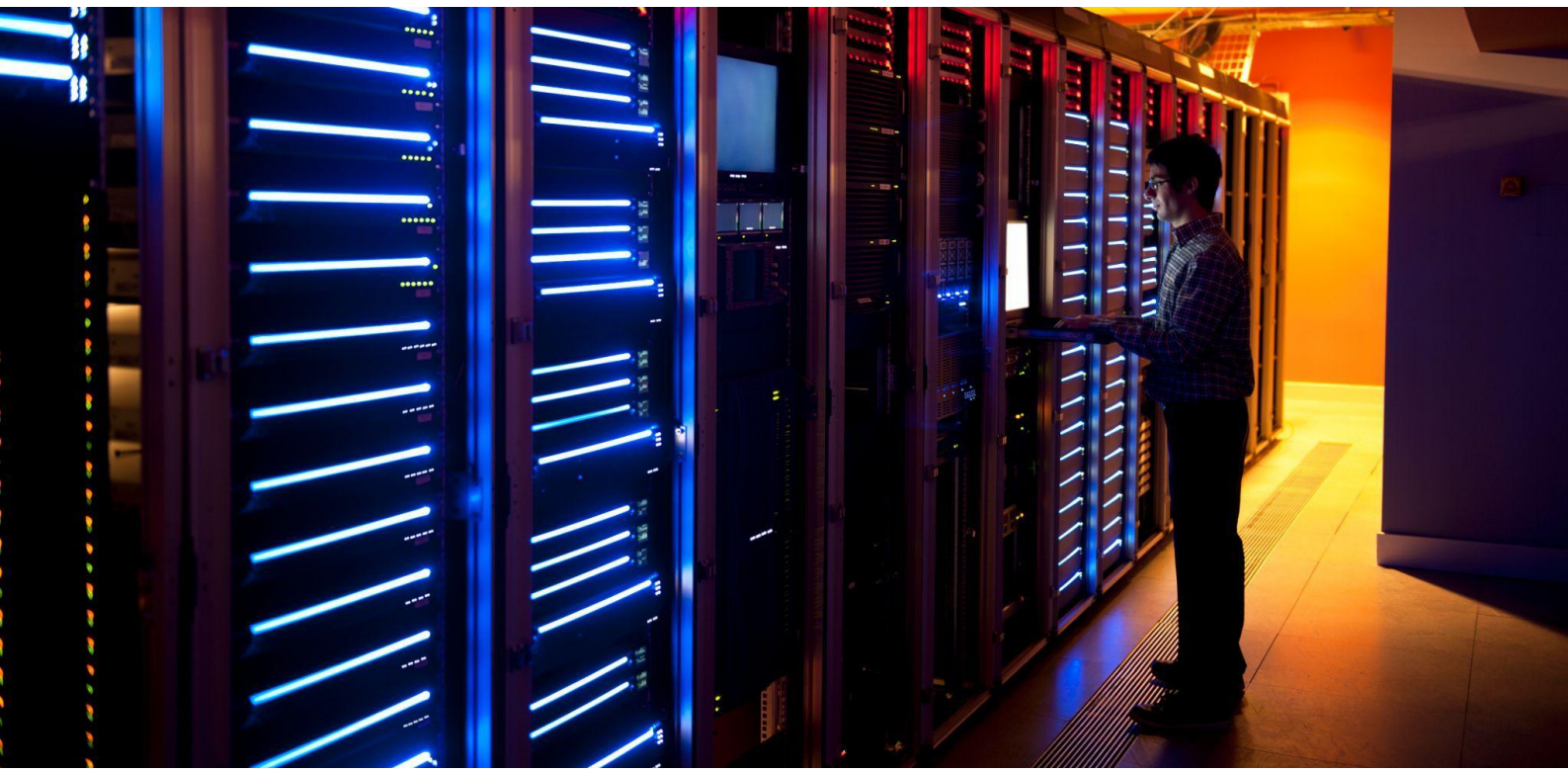
- **الموافقة** - تم تقديم الموافقة من صاحب البيانات على معالجة بياناته الشخصية.
- **البيانات المتاحة للعامة** - إذا كانت البيانات الشخصية متاحة للعموم، أو جرى جمعها من مصدر متاح للعموم.
- **المصلحة العامة** - إذا كانت جهة التحكم جهة عامة، وكان جمع البيانات الشخصية أو معالجتها مطلوبًا لأغراض المصلحة العامة أو لأغراض أمنية أو لتنفيذ نظام آخر أو لاستيفاء متطلبات قضائية.
- **المصالح الحيوية** - إذا كان عدم جمع أو معالجة البيانات الشخصية قد يضر صاحب البيانات أو يؤثر على مصالحه الحيوية.
- **الصحة والسلامة العامة** - إذا كان جمع البيانات الشخصية أو معالجتها ضروريًا لحماية الصحة العامة أو السلامة العامة أو حماية حياة فرد أو أفراد معينين أو حماية صحتهم.
- **البيانات التي خضعت لإخفاء الهوية** - إذا كانت البيانات الشخصية لن تُسجل أو تُحفظ في صيغة تجعل من الممكن تحديد هوية صاحبها ومعرفته بصورة مباشرة أو غير مباشرة.
- **المصالح المشروعة** - تكون معالجة البيانات الشخصية ضرورية لتحقيق مصالح مشروعة لجهة التحكم والتي لا تشمل البيانات الحساسة.

المسوغات النظامية للإفصاح عن البيانات الشخصية

بالإضافة إلى وجود مسوغ نظامي للمعالجة، يلزم وجود مسوغ نظامي منفصل في حالة الإفصاح عن البيانات الشخصية (مثل: الإفصاح عن البيانات الشخصية إلى جهة أخرى - بما في ذلك التي تكون داخل نفس مجموعة الجهات).

المسوغات النظامية للإفصاح[٨] عن البيانات الشخصية (المادة رقم ١٥ من النظام)

- **الموافقة** - تم تقديم الموافقة من صاحب البيانات على الإفصاح عن بياناته الشخصية.
- **البيانات المتاحة للعامة** - إذا كانت البيانات الشخصية قد جرى جمعها من مصدر متاح للعموم.
- **المصلحة العامة** - إذا كانت الجهة التي تطلب الإفصاح جهة عامة، وكان ذلك لأغراض المصلحة العامة أو لأغراض أمنية أو لتنفيذ نظام آخر أو لاستيفاء متطلبات قضائية.
- **الصحة والسلامة العامة** - إذا كان الإفصاح ضرورياً لحماية الصحة العامة أو السلامة العامة أو حماية حياة فرد أو أفراد معينين أو حماية صحتهم.
- **البيانات التي خضعت لإخفاء الهوية** - إذا كان الإفصاح سيقتصر على معالجتها لاحقاً بطريقة لا تؤدي إلى معرفة هوية صاحب البيانات الشخصية أو أي فرد آخر على وجه التحديد.
- **المصالح المشروعة** - إذا كان الإفصاح ضرورياً لتحقيق مصالح مشروعة لجهة التحكم، ما لم يخل ذلك بحقوق صاحب البيانات الشخصية أو يتعارض مع مصالحه ولم تكن تلك البيانات بيانات حساسة.



[٨] يرجى ملاحظة أنه في أي حال يجب على جهة التحكم الالتزام بالقيود المفروضة على الإفصاح، كما هو محدد في المادة رقم ١٦ من النظام.

حقوق أصحاب البيانات الشخصية

يوفر النظام للأفراد حقوقًا معينة فيما يتعلق بمعالجة بياناتهم الشخصية. حيث يجب على جهة التحكم تمكين الأفراد من ممارسة جميع هذه الحقوق بشكلٍ فعال.

	حق أصحاب البيانات	وصف الحق	مواد النظام
١	الحق في العلم	يحق للأفراد إحاطتهم علمًا بالمسوغ النظامي لجمع بياناتهم الشخصية والغرض من ذلك.	الفقرة ١ من المادة ٤
٢	الحق في الوصول إلى البيانات الشخصية	يحق للأفراد الوصول إلى بياناتهم الشخصية المتوفرة لدى جهة التحكم.	الفقرة ٢ من المادة ٤
٣	الحق في طلب الحصول على البيانات الشخصية	يحق للأفراد طلب تقديم نسخة من بياناتهم الشخصية بصيغة مقروءة وواضحة.	الفقرة ٣ من المادة ٤
٤	الحق في طلب تصحيح البيانات الشخصية	يحق للأفراد طلب تصحيح بياناتهم الشخصية إذا كانت غير صحيحة، أو إتمامها إذا كانت ناقصة، أو تحديثها إذا كانت غير محدثة.	الفقرة ٤ من المادة ٤
٥	الحق في طلب إتلاف البيانات الشخصية	يحق للأفراد طلب إتلاف بياناتهم الشخصية وفقًا لمتطلبات النظام واللوائح.	الفقرة ٥ من المادة ٤
٦	الحق في الرجوع عن الموافقة	يحق للأفراد في أي وقت الرجوع عن موافقتهم التي قدموها من قبل عن معالجة بياناتهم الشخصية.	الفقرة ٢ من المادة ٥
٧	الحق في تقديم شكوى إلى الجهة المختصة	يحق للأفراد تقديم شكوى إلى الجهة المختصة حول تنفيذ النظام واللوائح.	المادة رقم ٣٤

يجب على جهة التحكم تنفيذ طلبات صاحب البيانات المتعلقة بحقوقه وفقًا لنظام حماية **خلال مدة لا تتجاوز ٣٠ يومًا** ودون تأخير. ولها تمديد ذلك في حال تطلب التنفيذ جهدًا إضافيًا غير متوقع أو غير معتاد أو في حال تلقيها طلبات متعددة من صاحب البيانات الشخصية وذلك بما لا يزيد على ٣٠ يومًا إضافية، بشرط أن تُشعِر صاحب البيانات الشخصية مسبقًا بالتمديد ومبرراته.

ومن أجل الاستجابة بفعالية للحقوق المذكورة أعلاه، ينبغي أن يكون لدى جهة التحكم، على سبيل المثال، ما يلي:

- السياسة والإجراءات حول تنفيذ طلبات ممارسة حقوق أصحاب البيانات الشخصية.
- النموذج لتقديم طلبات ممارسة حقوق أصحاب البيانات الشخصية (ممكن لقنوات مختلفة).
- الفريق المتخصص والمدرب والقادر على تنفيذ طلبات ممارسة حقوق أصحاب البيانات الشخصية بفعالية.
- الأدوات التكنولوجية التي يمكن لفريق حماية البيانات الشخصية استخدامها لتنفيذ طلبات ممارسة حقوق أصحاب البيانات الشخصية.

التواصل معنا

يرجى 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

شكرًا لكم