الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

PERSONAL DATA PRIVACY PROTECTION LAW OVERVIEW

Law no. 13 of 2016

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

National Cyber Governance and Assurance Affairs, National Cyber Security Agency (NCSA), is the competent department Law No. I 3 of 2016; the Personal Data Privacy Protection Law (PDPPL)

National Cyber Governance and Assurance Affairs oversees the Personal Data Privacy Protection Law (PDPPL) and therefore regulates data privacy in the State of Qatar. It offers advice and guidance, promotes good practice, carries out audits and advisory visits, considers complaints, monitors compliance and supports enforcement action where appropriate.

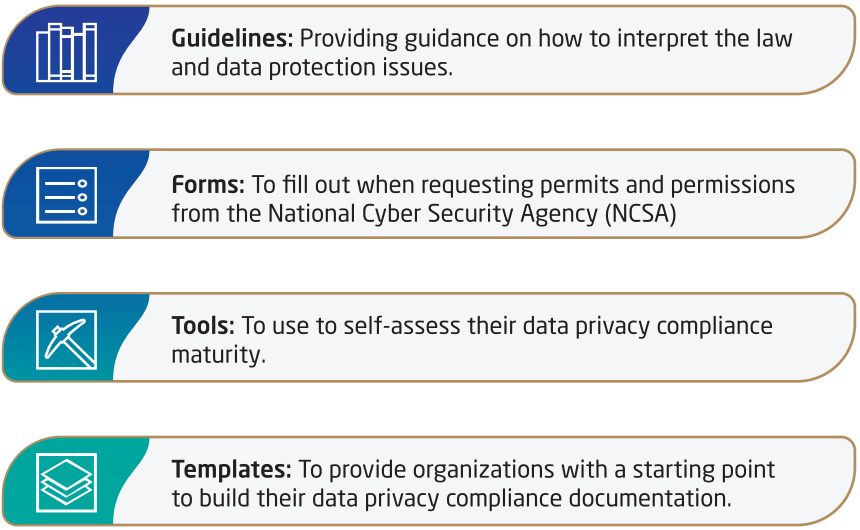
This booklet gives an overview of the main concepts of PDPPL.

Have you seen the PDPPL Guidance Hub?

The guidance hub contains guidelines for organizations in Qatar on their obligations under the the Personal Data Privacy Protection Law of 2016 (PDPPL)

What can you find on the guidance hub?

Organizations should assess their PDPPL compliance initiatives against these guidelines and take action to close any gaps they identify immediately.



https://compliance.qcert.org/ar/privacy/hub

What does the PDPPL mean for organizations?

In Qatar, organizations must comply with the Personal Data Privacy Protection Law of 2016 (PDPPL).
The PDPPL poses risks to organizations if they find themselves in non-compliance. It also provides opportunities to gain a competitive advantage through developing consumer trust

Key risks and opportunities that the PDPPL provides to organizations include:

Risk	Opportunities
Fines	Reduce chance of breach
Brand damage	Increased employee / consumer trust
Ineffective implementation	Increased protections

If organizations do not take action to mitigate risks and carry out compliance activities the NCSA may take a number of investigatory and / or enforcement actions.

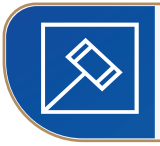
What are the individual rights?

In Qatar, the Personal Data Privacy Protection Law of 2016 (PDPPL) gives you a number of rights regarding your data

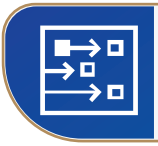
Individuals' rights under the PDPPL

The PDPPL enshrines a number of rights you have as an Individual regarding your personal data, in certain circumstances.

The right to protection and lawful processing



The right to request correction



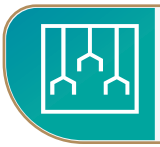
The right to withdraw consent

The right to be notified of processing

The right to erasure

The right to be notified of inaccurate disclosure

The right to object



The right to access

What does a data privacy programme look like?

Organizations must implement a data privacy programme to meet the requirements of Personal Data Privacy Protection Law (PDPPL)

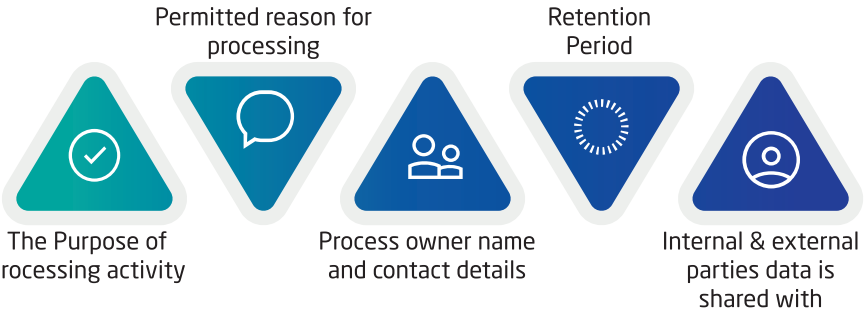
What are the key elements of a data privacy programme?

1. Vision and strategy
2. Identification and operationalization of appropriate administrative, technical and financial measures
3. Data privacy governance and operating model
4. Data processing records and impact assessments
5. Policies and procedures
6. Third party analysis and management
7. Regulatory engagement with the NCSA
8. Implementation of privacy by design and default and continuous improvement
9. Operationalization of business-as-usual compliance

Why is a Record of Processing Activities important?

A Record of Processing Activities (RoPA) provides an organization with a complete source of information on personal data processing including what personal data they process, how they process it and the controls in place to ensure it is processed in compliance with the PDPPL

Examples of what can be included in a RoPA?



1. Confirm requirements
2. Identify stakeholders
3. Document format decision
4. Brief stakeholders
5. Provide continuous support
6. Ongoing review

What precautions are appropriate to protect personal data ?

The Personal Data Privacy Protection Law (PDPPL) requires organizations that process personal data to have 'appropriate administrative, technical and financial precautions' in place to protect personal data

How to determine what measures are 'appropriate?'

Organizations should assess their PDPPL compliance initiatives against these guidelines and take actions to close any gaps they identify immediately.

Administrative precautions

Administrative precautions are those that relate to the management of their organization and the way they carry out tasks to deliver privacy.

Technical precautions

Technical precautions are those that relate to the use of technology to carry out tasks or achieve certain outcomes to deliver privacy.

Financial precautions

Financial precautions are those that relate to investment in products or services to carry out tasks or achieve certain outcomes to deliver privacy.

What are the third-party processors considerations?

When engaging a third party processor, the PDPPL requires controllers to verify that such processors comply with the instructions given to them, adopt appropriate precautions and monitor their compliance on a regular basis as part of their Personal Data Management System (PDMS).

With respect to a processing activity, an organization can play one or more of the following roles:

1. **A Controller** if it is the main decision-maker exercising overall control over why and how personal data is processed.
2. **A Processor** if it is following the instructions of a Controller or is processing personal data on their behalf.
3. **A Joint-Controller** if it jointly makes decisions or exercises shared control over why and how the personal data is processed.

What does the PDPPL say in regards to third-party processors?

1. Put in place legally binding responsibilities for the protection of personal data through a contract.
2. Assess processors compliance e.g. through a 'Procurement Questionnaire.
3. Investigate cross-border transfers taking place.

What do you need to consider about direct marketing?

Direct marketing involves the communication, by whatever means, of any advertising or marketing material which is directed to particular individuals, however nowadays it is largely carried out by organizations via electronic means.

Direct Marketing via electronic means requires

- Permitted reason
- Individuals' consent
- Record maintained for consent
- The right to withdraw consent anytime

Key considerations for direct marketing by a third party:

comply with obligations under the PDPPL implementing appropriate administrative, technical and financial precautions;

have signed a contract with the controller as a joint-controller or processor; and

make it clear to individuals that they are acting on behalf of the controller and that the controller is clearly identified as the originator.

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

PERSONAL DATA PRIVACY PROTECTION LAW OVERVIEW

Law No. 13 of 2016

Contact Us:

National Cyber Governance and Assurance Affairs

Postal address
National Cyber Governance and Assurance Affairs,
National Cyber Security Agency (NCSA),
P.O. Box 24100,
Wadi Al Sail Street,
Doha, Qatar

Privacy related inquiries:
Phone: (+974) 2362220
E-mail: privacy@ncsa.gov.qa

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

نظرة عامة على قانون حماية خصوصية البيانات الشخصية

قانون رقم ١٣ لعام ٢٠١٧

اتصل بنا

شؤون الحوكمة والضمان السيبرانى الوطني

العنوان البريدي
شؤون الحوكمة والضمان السيبرانى الوطني
الوكالة الوطنية للأمن السيبراني
صندوق بريد ٢٤١٠٠
شارع وادي السيل
الدوحة, قطر

للاستفسرات المتعلقة بحماية البيانات الشخصية:
هاتف: +٩٧٤ ٢٣٦٢٢٢٠
بريد الكتروني: privacy@ncsa.gov.qa

ما هي الاحتياطات المناسبة؟

يتضمن التسويق المباشر الاتصال عبر أي وسيلة كانت باستخدام مادة إعلانية أو تسويقية موجهة إلى أفراد بعينهم ,ويتم تنفيذ ذلك في الوقت الحاضر من قبل المؤسسات عبر الوسائل الإلكترونية.

التسويق المباشر عبر الوسائل الإلكترونية يتطلب:

- تحديد السبب الذي يسمح بمعالجة البيانات الشخصية
- موافقة الأفراد
- الاحتفاظ بسجل الموافقات
- إمكانية سحب الموافقة في أي وقت

الاعتبارات الرئيسية للتسويق عبر طرف ثالث:

الامتثال للالتزامات بموجب قانون حماية خصوصية البيانات الشخصية PDPPL مع تنفيذ الإجراءات الإدارية والفنية والمالية المناسبة

توقيع عقد مع المراقب كمراقب مشترك أو معالج

توفير توضح للأفراد بأنهم يتصرفون نيابة عن المراقب وأن المراقب محدد بوضوح باعتباره المنشي لعملية المعالجة.

ما هي الاعتبارات المتعلقة بمعالج البيانات كطرف ثالث؟

عند إشراك معالج ما كطرف ثالث، يتطلب قانون حماية خصوصية البياناتPDPPL من المراقب التحقق من امتثال المعالج المكلف للتعليمات الموجهة له، واعتماد الإجراءات المناسبة ومراقبة امتثاله على أساس منتظم كجزء من نظام إدارة البيانات الشخصية (PDMS)

فيما يتعلق بنشاط معالجة البيانات، فإن المؤسسة تقوم بدور أو أكثر من الأدوار التالية:

١

مراقب

إذا كانت صانع القرار الرئيسي الذي يمارس السيطرة الشاملة على سبب وكيفية معالجة البيانات الشخصية.

٢

معالج

إذا كانت تتبع تعليمات مراقب أو تعالج البيانات الشخصية نيابة عنه.

٣

مراقب مشترك

إذا كانت تتخذ قرارات مشتركة أو تمارس السيطرة مشتركة على السبب وكيفية معالجة البيانات الشخصية.

ماذا الذي ينص عليه قانون حماية خصوصية البيانات الشخصية PDPPL فيما يتعلق بمعالج البيانات كطرف الثالث؟

١ وضع مسؤوليات ملزمة قانونا لحماية خصوصية البيانات الشخصية من خلال إبرام عقد.

٢ تقييم امتثال معالج البيانات على سبيل المثال: من خلال "استبيان لمزودي الخدمات."

٣ التحقيق في عمليات نقل البيانات التي تحدث عبر الحدود.

ما هي الاحتياطات المناسبة لحماية البيانات الشخصية؟

يتطلب قانون حماية خصوصية البيانات الشخصية (PDPPL) من المؤسسات التي تعالج البيانات الشخصية أن يكون لديها " الاحتياطات الإدارية والفنية والمالية المناسبة " لحماية البيانات الشخصية.

كيف يمكن تحديد الإجراءات "المناسبة"؟

يجب على المؤسسات تقييم مبادرات الامتثال لقانون حماية خصوصية البيانات الشخصية PDPPL الخاصة بها وفق المبادئ التوجيهية واتخاذ إجراءات لسد أي ثغرات تحددها على الفور.

الاحتياطات إدارية

الاحتياطات الإدارية هي تلك التي تتعلق بإدارة المؤسسة والطريقة التي تنفذ بها المهام المناسبة لحماية البيانات الشخصية.

الاحتياطات الفنية

الاحتياطات التقنية هي تلك التي تتعلق باستخدام التكنولوجيا لتنفيذ المهام أو تحقيق نتائج معينة لتوفير الحماية المناسبة للبيانات الشخصية.

الاحتياطات المالية

الاحتياطات المالية هي تلك التي تتعلق بالاستثمار في المنتجات أو الخدمات التنفيذ المهام أو تحقيق نتائج معينة لتوفير الحماية المناسبة للبيانات الشخصية

ما هي أهمية سجل أنشطة معالجة البيانات الشخصية؟

سجل أنشطة معالجة البيانات الشخصية (RoPA) يوفر للمؤسسات مصدرا كاملة للمعلومات حول معالجة البيانات الشخصية بما في ذلك البيانات الشخصية التي يتم معالجتها وكيفية معالجتها وعناصر التحكم المطبقة لضمان معالجتها وفقاً القانون حماية خصوصية البيانات الشخصية.PDPPL

أمثلة على ما يمكن تضمينه في سجل أنشطة معالجة البيانات الشخصية RoPA ؟

١ تأكيد المتطلبات

٢ تحديد أصحاب المصلحة

٣ قرار تنسيق الوثائق

٤ إطلاع أصحاب المصلحة

٥ تقديم الدعم المستمر

٦ المراجعة المستمرة

ما هي العناصر الأساسية التي يشتمل عليها برنامج حماية خصوصية البيانات؟

يجب على المؤسسات تنفيذ برنامج حماية خصوصية البيانات لتلبية متطلبات قانون حماية خصوصية البيانات الشخصية (PDPPL)

١ الرؤية والاستراتيجية

٢ تحديد وتطبيق الإجراءات الإدارية والفنية والمالية المناسبة

٣ حوكمة حماية خصوصية البيانات ونموذج التشغيل

٤ سجلات معالجة البيانات وتحليلات تأثير حماية خصوصية البيانات الشخصية

٥ السياسات والإجراءات

٦ تحليل وإدارة الطرف الثالث

٧ المشاركة التنظيمية مع الوكالة الوطنية للأمن السيبراني

٨ التطبيق والتحسين المستمر لحماية خصوصية البيانات المتضمنة بالتصميم والمتضمنة افتراضيا

٩ الامتثال لإجراء الأنشطة والعمليات بالشكل الاعتيادي للأعمال

ما هي الحقوق التي يشتمل عليها قانون حماية خصوصية البيانات الشخصية؟

يشتمل قانون حماية خصوصية البيانات الشخصية PDPPL على عدد من الحقوق التي يتمتع بها الفرد فيما يتعلق بالبيانات الشخصية، في ظروف معينة.

- الحق في حماية البيانات الشخصية ومعالجتها بشكل مشروع
- حق طلب تصحيح البيانات الشخصية
- الحق فى سحب الموافقة السابقة على معالجة البيانات الشخصية
- حق الإخطار بمعالجة البيانات الشخصية
- حق الحذف
- حق الإخطار بأي إفشاء بيانات شخصية غير دقيقة
- حق الاعتراض
- حق في الوصول للبيانات الشخصية

ماذا يعني قانون حماية خصوصية البيانات الشخصية بالنسبة للمؤسسات؟

في دولة قطر، يجب على المؤسسات الامتثال لقانون حماية خصوصية البيانات الشخصية (PDPPL) لعام ٢٠١٦.
يشكل عدم الامتثال لقانون حماية خصوصية البيانات الشخصية PDPPL مخاطر على المؤسسات. بينما يوفر الامتثال للقانون فرصا لاكتساب ميزة تنافسية من خلال تطوير ثقة المستهلكين والعملاء.

المخاطر	الفرص
الغرامات المالية	تقليل فرصة الاختراقات
التأثير السلبي على العلامة التجارية والسمعة	زيادة ثقة الموظفين / المستهلكين
التطبيق غير الفعال للقانون	زيادة حماية خصوصية البيانات

إذا لم تتخذ المؤسسات إجراءات للتخفيف من المخاطر وتنفيذ أنشطة الأمتثال، فقد تتخذ الوكالة الوطنية للأمن السيبراني عددا من إجراءات التحقيق و/أو الإنفاذ

ما الذي تعرفه عن دليل المبادئ التوجيهية الخاص بقانون حماية خصوصية البيانات الشخصية PDPPL؟

يحتوي دليل المبادئ التوجيهية على المبادئ التوجيهية للمؤسسات في دولة قطر بشأن الالتزام بموجب قانون حماية خصوصية البيانات الشخصية (PDPPL) العام ٢٠١٦

ماذا يقدم دليل المبادئ التوجيهية؟

يجب على المؤسسات تقييم مبادرات الامتثال لقانون حماية خصوصية البيانات الشخصية PDPPL الخاصة بها تجاه هذه للمبادئ التوجيهية واتخاذ إجراءات مناسبة لسد أي ثغرات يتم تحديدها على الفور.

- **المبادئ التوجيهية :** لتقديم المبادم التوجيهية فيما يخص كيفية تفسير القانون وقضايا حماية خصوصية البيانات.
- **النماذج:** لملتها عند طلب التصاريح والأذونات تتخذ الوكالة الوطنية للأمن السيبراني.
- **الأدوات :** لاستخدامها في التقييم الذاتي لمستوى نضج امتثال حماية خصوصية البيانات لدى المؤسسة.
- **نماذج الوثائق :** لتزويد المؤسسات بنقطة بداية لبناء وثائق الامتثال الخصوصية البيانات الخاصة بهم.

https://compliance.qcert.org/ar/privacy/hub

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

تعتبر شؤون الحوكمة والضمان السيبرانى الوطني بالوكالة الوطنية للأمن السيبراني المختصة بتنظيم القانون رقم ١٣ لسنة ٢٠١٦ المعروف أيضا باسم قانون حماية خصوصية البيانات الشخصية (PDPPL).

تشرف شؤون الحوكمة والضمان السيبرانى الوطني بالوكالة الوطنية للأمن السيبراني على تنظيم القانون وبالتالي تنظم حماية خصوصية البيانات بدولة قطر. تقدم شؤون الحوكمة والضمان السيبرانى بالوكالة الوطنية للأمن السيبراني الوطني المنشورة والتوجيه، وتعزز الممارسات الجيدة، وتقوم بعمليات التدقيق و الزيارات الاستشارية، والنظر في الشكاوي، وتراقب الامتثال، وتدعم اجراءات الانفاذ عند الاقتضاء.

تقدم هذه النشرة التوعوية نظرة عامة على أهم المفاهيم والمبادئ الخاصة بقانون حماية خصوصية البيانات الشخصية.

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

نظرة عامة على قانون حماية خصوصية البيانات الشخصية

قانون رقم ١٣ لعام ٢٠١٧