KensingtonSwan

If GDPR applies to your business–what should you do?

The EU General Data Protection Regulation 2016/679 (GDPR) applies from 25 May 2018. The first thing for non-EU businesses to consider is whether any of your business is within the general scope of the GDPR. It applies to the processing of personal data:

- in the context of the activities of an establishment of a Controller or a Processor in the EU, whether or not the processing takes place in the EU; or
- of data subjects who are in the EU by a Controller or Processor not established in the EU where the processing relates to the offering of goods or services (whether free or paid for), or the monitoring of behaviour, which takes place within the EU.

If GDPR applies to your business and you're not sure where to start, start here for guidance on what Controllers need to do. Then get in contact with us to help you comply.

Do you know what Data you have?

You need to Map/Audit your data comprehensively and implement and maintain processes for updating this.

Understand what laws apply to your data

Understand if GDPR applies to you and to what extent.

Do you need to appoint a Data Protection Officer? If so they need to be suitable

Yes if a public authority or if your core activities require: i) large scale, regular and systematic monitoring of individuals; or ii) large scale processing of special categories of data.

Clarify and understand the legal basis of processing

At least one of these must apply: Consent; Contract; Legal obligation; Vital interests; Public task; Legitimate interests.

Governance awareness and Update Policies and Procedures

Integrate privacy compliance into the audit framework and train staff.

Third Party Relationships and Data Transfers

Are all third party relationships and data transfers adequately disclosed in your privacy notice(s)? You will need to include specific things in your contracts and comply with requirements to safeguard the information.

Plan for data breach –Duty to notify data breaches

You need procedures in place to identify, report and investigate breaches within 72 hours.

Understand and update your current Privacy Policies and Notices

Check that they are up to date and include necessary provisions for GDPR.

International considerations

If no EU presence, you may need to appoint a local representative in the EU.

Protection of children

Put systems in place to verify individuals' ages and to obtain parental or guardian consent.

How are you obtaining consent?

GDPR requires: A 'Positive opt-in'; Records of consent; Ability for individuals to withdraw consent.

Do you do any automated decision making and profiling?

Check it is compliant. Be prepared to share your processes on this, and have a plan for human intervention if requested.

Privacy impact assessments (PIAs)

Recognise high risk data and processes.

Privacy by design

Privacy considerations and processes need to be embedded in all your major projects.

The GDPR Toolkit for New Zealand Businesses.

What are some of the things you need to do?

What Data have you got? Map/Audit your data

Identify all data processed in a detailed Record of Processing including a comprehensive data flow map.

Consider:

- What data is being held? Be reasonably specific in your description of categories of data. Is any of it considered sensitive?
- Where did it come from and under what terms/consent?
- Where is the data being held/stored?
- Who is responsible for managing the data?
- What is the data being used for (i.e. the purpose of processing)?
- Is the data up to date? How do you know this?
- Is it necessary to still be holding/processing the data?
- Who has access to the data?
- Who do you share it with?
- What security is in place to protect the data? How secure is it? Do you test your security?
- Can it be accessed and provided should an access request be received?

Implement and maintain processes for updating and maintaining this Record of Processing.

Understand what laws apply to your data

Understand the implication (if any) of GDPR on your non-EU business.

If you currently conduct criminal records checks in the EU, review national laws to ensure you can continue to do so.

Privacy Policies and Notices

Where are they and what do they relate to? Are the reflective of reality and the data mapping/audit you have done?

Are they appropriate for all laws that might apply? NZ? Australia? GDPR?

Under the GDPR there are some additional things you will have to tell people. Such as explaining your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to an appropriate Data Protection Authority if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language and the level of detail and specifics appears higher than NZ standard practice.

Clarify the legal basis of processing

Identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Legal obligation: the processing is necessary for a controller to comply with the law.

Vital interests: the "processing is necessary in order to protect the vital interests of the data subject or of another natural person".

Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Under the GDPR, privacy notices must state the processing ground relied upon, and if relying on legitimate interests, state the nature of the legitimate interest.

If special category (sensitive) data, including race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation data is processed, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9 (of which there are 10 options).

Governance awareness and Update Policies and Procedures

Document your Privacy Governance Model. Ensure clear roles and responsibilities and reporting lines to embed privacy compliance into the organisation and have appropriate documentation to be able to demonstrate how you are complying with GDPR. Integrate privacy compliance into the audit framework and train staff.

Have clear processes and procedures to comply with requests for access, correction and deletion. Ensure technical and operational processes are in place to ensure data subjects' rights can be met, e.g. right to be forgotten, data portability and the right to object. How would you delete personal data or provide data electronically and in a commonly used format. Would your systems help you to locate and delete the data? Who will make the decisions about deletion?

Data Protection Officer

Do you need to appoint a data protection officer (**DPO**)? The GDPR introduces a duty to if:

- you are a public authority (except for courts acting in their judicial capacity);
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

A DPO must be fully conversant in what is covered by the GDPR, and how it affects the business and they need to be independent from data decisions. They also need to be able to create and manage data protection systems and processes.

Plan for data breach—Duty to notify data breaches

Under GDPR you will need to notify data breaches to an appropriate Data Protection Authority where the individuals concerned are likely to suffer harm. It is therefore important to have procedures in place to identify, report and investigate breaches within 72 hours.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

If you have data of other non-EU individuals consider whether other mandatory reporting requirements apply to this data.

Third Party Relationships and Data Transfers

Consider all third party relationships:

- Are you a data processor for a third party?
- Do you contract with service providers who will therefore be deemed processors?
- Identify all cross-border data flows. You should only transfer data outside of the EU to countries that offer an appropriate level of protection.

Consider whether you need to add provisions to contracts. Develop compliant contract wording for customer agreements and third-party service provider agreements.

Are all third party relationships and data transfers adequately disclosed in your privacy notice(s)?

Protection of children

Identify whether you process personal data of children. GDPR brings in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If so:

- put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity;
- ensure that notices directed at that child are "child-friendly" and if consent is relied upon, you have implemented a mechanism to seek parental consent.

International considerations

If no EU presence, you may need to appoint a local representative in the EU.

If your organisation operates in more than one EU member state, you should determine your lead Data Protection Authority and document this.

Privacy by design

Ensure processes are in place to embed privacy by design into projects (e.g. technical and organisational measures are in place to ensure data minimization, purpose limitation and security).

Automated decision making and profiling

The GDPR, generally applies to, and has specific provisions relating to:

- automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them. You can only carry out this type of decision-making where the decision is necessary for the entry into or performance of a contract or based on the individual's explicit consent. You must also:

- give individuals information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision; and
- carry out regular checks to make sure that your systems are working as intended.

Privacy impact assessments (PIAs)

You must do a data protection impact assessment (**DPIA**) for certain listed types of processing, or any other processing that is likely to result in **a high risk** to individuals' interests e.g. for projects that involve processing, on a large scale, of sensitive personal data or criminal convictions, monitoring of a public area or systematic and extensive evaluation by automated means including profiling.

The focus is on the 'residual risk' after any mitigating measures have been taken. If you have carried out a DPIA that identifies a high risk, and you cannot take any measures to reduce this risk, you need to consult with the relevant Data Protection Authority. You cannot go ahead with the processing until you have done so.

How are you obtaining consent?

Under GDPR, consent must be freely given, specific, informed and unambiguous. You should review how you seek, record and manage consent and whether you need to make any changes.

- Consent means offering individuals real choice and control.
- There must be a positive opt-in, consent cannot be inferred from silence, pre-ticked boxes or inactivity. It also requires individual ('granular') consent options for distinct processing operations. Your customers will need to be able to select those that they agree with and decline those they do not like, and you need to be able to store your customer's preferences in your databases. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.
- You must keep clear records to demonstrate consent. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data.
- The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time. Consent can be withdrawn at any time and systems must be able to handle withdrawal requests.

Where consent is relied upon as the ground for processing personal data, review existing consents to ensure they meet the GDPR requirements, and if not implement a process to seek new consents.

We can help with your compliance process.

Hayley Miller
PARTNER
hayley.miller@kensingtonswan.com
DDI +64 9 915 3366 | M +64 21 870 477

Campbell Featherstone
SENIOR ASSOCIATE
campbell.featherstone@kensingtonswan.com
DDI +64 4 498 0832 | M +64 21 809 779