BUDDLE FINDLAY

GDPR and the Privacy Bill: Mind the gap

Allan Yeoman, Amy Ryburn, Philip Wood, Renee Stiles, Alex Chapman, Damien Steel-Baker, Keri Johansson

18 November 2019

With the new Privacy Bill likely to be implemented in a little over six months and the Christmas break looming, it's a good time for agencies to consider what the new Privacy Bill (Bill) means for them. A recap on the changes introduced by the Bill is available in our article 'Privacy Bill – Five changes to watch out for'.

For those organisations who may be subject to both the new Bill (once enacted) and the European Union's General Data Protection Regulation (GDPR), it will be particularly important to understand not only how the Bill differs from both the current Privacy Act 1993 (Act), but also the GDPR.

At a glance

Both the GDPR and the Bill apply a number of broadly similar principles, which form the basis on which personal information can be processed. However, the Bill and the GDPR are materially different and compliance with the Bill does not mean compliance with the GDPR. In summary of the more material gaps between the Bill and the GDPR (which are expanded on in the table below), the GDPR:

- Generally takes a more prescribed and detailed approach to the treatment of personal information (which seems necessary given the European Union's intent to harmonise data privacy laws across the various different approaches taken by the member countries within the European Union)
- Applies to a wider range of information
- Imposes obligations on agents (or processors), even where those agents only act in accordance with the agency's obligations
- Imposes a number of requirements regarding the basis on which an individual's consent can be relied on
- Has a lower threshold for breach notifications
- Includes additional rights for individuals, such as rights to erasure and data portability
- Imposes express record keeping obligations on agencies
- Has considerably greater maximum fines.

While there are some material differences between the Bill and the GDPR, in our view, recent commentary (as summarised in our previous articles here and here) on the Bill by the Privacy Commissioner (Commissioner), indicates that the Bill (once enacted) will be interpreted and applied by the Commissioner in a manner that is more aligned with the GDPR. This approach is likely to be particularly important in the context of the European Commission's review into whether New Zealand's privacy laws continue to provide an adequate level of data protection to that in the European Union. If our privacy laws are no longer considered to be "adequate" by the European Commission then the free flows of data that we currently enjoy with the European Union will come to an end, which may mean more administrative "red tape" for businesses that transact with Europe.

Mind the gap

The more material gaps between the GDPR and the Bill are summarised below:

GDPR	THE PRIVACY BILL
PERSONAL DATA AND PERSONAL INFORMATION	
The GDPR relates to the processing of "personal data", which is defined broadly to mean any information relating to an identified or identifiable natural person and includes a natural person who can be identified directly or indirectly, for example by a name, identification number, location data, or	"Personal information" is defined in the Bill to mean information about an identifiable individual. While this definition of personal information is comparatively less comprehensive than the definition of personal data in the GDPR, in our view, the Commissioner's Office (OPC) is

one or more factors specific to the physical, physiological, genetic, mental, economic or social identity of that natural person. The GDPR also includes the concept of "special categories" of personal data, which includes, for example, personal data revealing racial or ethnic origin, genetic and biometric data for the purpose of identifying a natural person or data concerning health. The default position under the GDPR is that special categories of personal data should not be processed, unless that processing meets certain criteria, such as: • Where the relevant person has provided explicit consent (which is a higher standard of consent to that specified elsewhere in the GDPR, as summarised in the consent section below) or • In the context of employment arrangements.	likely to interpret the definition of personal information broadly so that the outcome may be quite similar to that under the GDPR. In relation to special categories of personal data, while Information Privacy Principle (IPP) 4 (when read alongside the OPC's guidance on that IPP) means that agencies should have regard to the nature of the personal information collected (eg whether the information is sensitive), the Bill does not include any express obligations to treat sensitive information (such as health or biometric data) any differently to more generic personal information.
CONTROLLERS AND PROCESSORS	
The GDPR has concepts of "controllers" (those who determine the purposes and means of the processing of personal data) and "processors" (those who process personal data on behalf of and as instructed by the controller). While most of the obligations under the GDPR are focused on controllers, processors also have liability in their own right. For example, processors must take reasonable steps to secure data (such as through encryption and pseudonymization) and must notify the controller without undue delay upon become aware of data breaches. In addition, the GDPR prescribes certain matters that must be addressed by way of contract between the controller and the processor.	While the Bill has clarified that sharing personal information with an agent will not constitute a disclosure for the purposes of the Bill (as summarised here), it does not otherwise make a distinction between controllers and processors. Instead, the Bill applies on a general basis to all agencies in, or carrying on business in, New Zealand, regardless of the scope of their operations or control over the relevant personal information. This means that agencies need to ensure that they comply with the terms of the Bill and, to the extent that they share personal information with agents, that those agents make appropriate contractual commitments regarding their use of such information.
CONSENT	
The GDPR states that processing of personal data shall only be lawful if and to the extent that the processing satisfies certain criteria. One such criterion is that the relevant individual has given consent to the processing of its personal data for one or more specific purposes. Any such consent will only be valid if it is specific, freely given by a clear affirmative act, informed, unambiguous and, where given in writing, it is presented in a manner that is clearly distinguishable from other matters (ie it should be separate from other terms), using clear and plain language. The controller must also be able to demonstrate that consent has been given on this basis. The individual must also be able to withdraw consent easily at any time.	The Bill reflects that processing of personal information may be authorised by the relevant individual in certain circumstances. For example, an individual may authorise an agency to use information for a purpose for which that information was not originally obtained. However, the Bill does not provide any express requirements about what will constitute valid authorisation or how that authorisation should be provided. However, the commentary provided by the Commissioner and his office suggests that "authorise" may be interpreted in a way that is closer to the standard of consent imposed by the GDPR, such that an individual's consent or authorisation under the Bill will only be valid where it is meaningful and the relevant individual has an option to withhold that authorisation.
BREACH NOTIFICATION	
Controllers must, without undue delay and, where feasible, within 72 hours of becoming aware, notify the competent supervisory authority of a personal data breach, unless the	As summarised here, under the Bill, agencies must notify the Privacy Commissioner and the affected individual(s) as soon as practicable after becoming aware of a notifiable

relevant breach is unlikely to result in a risk to the rights and freedoms of individuals. This is a relatively low threshold for notification as the default position is that controllers must notify the relevant supervisory authority of personal data breaches. Processors must also notify controllers without undue delay after becoming aware of a personal data breach. Where a personal data breach is likely to result in a "high risk" to the rights and freedoms of individuals, the controller must communicate that breach to the relevant individuals without undue delay. Notification to the individual will not be required if the relevant data is subject to appropriate technical and organizational measures that render it unintelligible (for example, encryption), the controller has taken steps which mean that the high risk to the rights and freedoms of data subjects is no longer likely to materialize or it would involve disproportionate effort (in that case, there would need to be some other public communication).	privacy breach. The breach notification provisions in the Bill have a higher notification threshold than that in the GDPR, which is helpful in that it is likely to decrease the over reporting of breaches. However, there is no obligation on an agency's own agent to notify the agency of any breach, so agencies will need to ensure that their agents are required to notify them of breaches by way of contract.
INDIVIDUAL'S RIGHTS	
In addition to broad rights of access and correction of personal data, under the GDPR, individuals have rights to: • Have their personal data erased (the "right to be forgotten") • Restrict the processing of their personal data (eg so that the data is made temporarily unavailable) • Not be subject to a decision based solely on automated processing, including profiling, where that processing produces legal effects which may significant affect them • "Data portability", which means that individuals have a right to receive the personal data they have provided to the controller in a "commonly used and machine readable format" and to have that data transmitted to another controller and • Object to processing of their personal data in certain circumstances.	The Bill includes rights for individuals to access and request correction of their personal information, but, despite the OPC's submissions on the Bill, it does not otherwise address the broader rights for individuals included in the GDPR. While there are a number of caveats in the GDPR to the application of individuals' rights, in our view, there is a clear gap between the GDPR and the Bill in this regard. However, it is useful to note that the Article 29 Data Protection Working Party has previously stated that the non-existence of data portability and restriction of processing rights should not be an obstacle for a country to be recognised as having equivalence with the EU framework (although they would be considered to be a "plus").
The GDPR includes express data and privacy management obligations, including: • An obligation to undertake data protection impact assessments where the relevant processing is likely to result in a high risk to rights and freedoms of natural persons • To appoint a data protection officer where, for example, the controller or processor's core activities consist of processing of the regular and systematic monitoring of individuals and • To undertake privacy "by design and by default", so it is mandatory to build privacy concerns into new systems, processes, services and products.	The Bill requires agencies to appoint privacy officers (as was the case under the Act). While the Bill does not include express obligations on agencies to undertake data protection impact assessments or to undertake privacy by design and by default, in any event, we consider that these practices are best practice and should be implemented by agencies in New Zealand.
RECORDS	
	The Bill does not include express obligations in relation to

Controllers must maintain a record of their data processing activities. Such records must include, in respect of all processing activities, records of the purposes of the processing, the categories of personal data and the technical and organisational security measures which are in place. Processors also have record retention obligations under the GDPR (although these are more limited obligations than those on controllers). In addition, controllers must be able to demonstrate that they comply with the general data protection principles in the GDPR, for example that they comply with the principles of lawfulness, fairness and transparency, purpose limitation and data minimisation.	records. However, in our view, such records are best practice and will be required to ensure that agencies can demonstrate to the Commissioner that they are using personal information in a way that is consistent with the Bill.

FINES	
The maximum fines under the GDPR total €20m or, in the case of an undertaking (ie a group of companies), four per cent of total worldwide annual turnover (whichever is higher).	The maximum payable fine under the Bill is $10,000.

Auckland

188 Quay Street
Auckland 1010

PO Box 1433
Auckland 1140
New Zealand

P: +64 9 358 2555
F: +64 9 358 2055

Wellington

Aon Centre
1 Willis Street
Wellington 6011

PO Box 2694
Wellington 6140
New Zealand

P: +64 4 499 4242
F: +64 4 499 4141

Christchurch

83 Victoria Street
Christchurch 8013

PO Box 322
Christchurch 8140
New Zealand

P: +64 3 379 1747
F: +64 3 379 5659