Data Protection Transition Period & Staff Data

What the end of the transition period means for Guernsey employers and staff data

The transition period

By 25 May 2018, when Guernsey's new data protection legislation was introduced, Guernsey businesses had done much to ensure that their personal data use complied with the new legislation. Acknowledging that at the time the new law took effect many businesses held large amounts of personal data, a year-long transition period was given for several of the more complicated areas of the new law. The transitional period ends on 25 May 2019.

While the processing of any new data, or processing of old data in a new way, must be in compliance with the new law, the transitional period was granted so that controllers (in this article, employers) could put in place measures to ensure that the personal data they held before May 2018 (and that they continued to process in exactly the same way) was processed in compliance with the new law. This is in contrast to the General Data Protection Regulation (GDPR) which had no transition period.

The complicated areas granted this grace period relate to (a) the employer's notification duties, (b) the validity of 'old' consents, (c) the duties of joint controllers, (d) the obligation to undertake impact assessments (DPIAs) and (e) the duties of processors. Additionally, the data subject right of 'portability' remains in the wings until the end of the transition period.

With the end of the transition period nearly upon us, Guernsey businesses should be looking at the data they held on 25 May 2018 to ensure that, by 25 May 2019, it is being processed lawfully and that the employer can respond to any staff member[1] exercising his or her rights.

The seven data protection principles will be familiar to most readers and, when considering the transitional provisions, these principles must be kept in mind

Notification

The employer must notify staff (i) of the identity of the controller processing their data (in many cases this will simply be the name of the employer but it may also include other group companies as joint controllers) as well as (ii) details as to what is done with their data. This is generally done by using privacy notices (also called fair processing statements) but notification can be done in other ways.

If the employer had personal information about staff before the new law took effect, and has continued to process the staff data in exactly the same way, then the employer has until the end of the

1 While this article refers to staff data, an employer may well have information about other people connected with staff, for example next of kin or dependents, and those other people are 'data subjects' and the law gives them the same protection as it gives to staff.

transition period to provide its privacy notice to all staff members.

It is worth noting that any new staff members or job applicants who provided personal information to the employer after 25 May 2018 must be (or have been) provided with the privacy notice either at the time the information was collected or, where the information was collected from a third party such as a recruitment agency, then within one month of when the data was first processed by the employer or transferred by the employer to a third party (whichever happens first). The transitional period has no effect on this 'new' data.

'Old' consents

Historically many staff members were asked to give their consent to the employer processing their personal data and many employment contracts contain a 'data protection consent' clause. The rules around what constitutes valid consent have changed and became more restrictive with introduction of the new law. In order for consent to be valid going forward, the employer must show that the consent was freely given having been based on clear and unambiguous information about how the data would be used. This means there must be no adverse effects for the individual if they decline to give that consent. This need for consent to be 'freely given' causes a problem in the employment context. In all but a few instances, an employer will no longer be able to rely on a staff member's consent as the lawful basis on which to process that individual's data.

Where an employer was processing a staff member's data on 25 May 2018 and was relying on his or her consent to do so (and provided that consent was valid under the old law) then that consent remains valid and only until the end of the transition period.

In the employment context there are other, better, grounds on which an employer can rely in order to lawfully process staff data both now and after 25 May 2019. Those grounds should be set out in the privacy notice and will mean that the falling away of the consent should not cause difficulty for employers in most cases.

Joint controllers

Where an employer shares staff data with another organisation and they both use the same personal data for the same purposes then they are 'joint controllers' of this data. (This is different from where the employer passes information to another organisation that uses the information for a purpose that is not identical to the purpose for which the employer uses the data. In that case the other organisation would simply be a 'further controller' and not a joint controller). Joint controller arrangements can occur in group company structures where staff are engaged via an employing company but other companies in the group use employee information, for example to make recruitment decisions, to decide the terms of the employee's engagement or the termination of the employment.

Where a true joint controller situation exists, the new law introduced new obligations on the joint controllers. Joint controllers must precisely define how the data is used to ensure it is protected, designate a primary point of contact for data subjects (the staff), set out each party's responsibilities and also specify the support to be provided to each other when a staff member (the data subject) exercises his or her rights or the Data Protection Authority asks for information.

The transitional period suspended these obligations in respect of data collected prior to 25 May 2018. In reality, as the obligation currently exists in respect of newly collected data (ie collected since 25 May 2018) then the necessary agreement should have been reached already and documentation put in place meaning extending this to cover the 'older' staff data should be relatively easy.

Impact Assessments (DPIAs)

The new law provides that an employer must not undertake any processing that poses a high risk to the legal rights and freedoms of staff unless it has undertaken a DPIA in respect of that processing. While the law gives examples of when a DPIA must be undertaken, it also imposes as more general obligation on the employer to think about the nature, scope, context and purposes of the processing and consider if the employer's contemplated processing would present a high risk to the staff member's legal rights or freedoms. The collective guidance on this is clear; if a controller is in doubt whether or not to undertake a DPIA then the DPIA should be undertaken. The EU's Data Protection Board has indicated that an employer should be undertaking a DPIA whenever it is intending to process the special category data of its employees. The Guernsey Data Protection Authority has provided a suggested template for a DPIA (www.odpa.gg).

Impact Assessments (DPIAs)

The new law provides that an employer must not undertake any processing that poses a high risk to the legal rights and freedoms of staff unless it has undertaken a DPIA in respect of that processing. While the law gives examples of when a DPIA must be undertaken, it also imposes as more general obligation on the employer to think about the nature, scope, context and purposes of the processing and consider if the employer's contemplated processing would present a high risk to the staff member's legal rights or freedoms. The collective guidance on this is clear; if a controller is in doubt whether or not to undertake a DPIA then the DPIA should be undertaken. The EU's Data Protection Board has indicated that an employer should be undertaking a DPIA whenever it is intending to process the special category data of its employees. The Guernsey Data Protection Authority has provided a suggested template for a DPIA (www.odpa.gg).

Where, on 25 May 2018, an employer was undertaking processing in respect of which a DPIA must be undertaken then the employer has until the end of the transition period to complete that DPIA.

Processors

We are regularly seeing confusion as to whether a business is acting as a controller or a processor. If a business decides how the data in question is used or processed then it is a controller of that data.

Relatively few businesses in Guernsey act as processors and an example of a true processor would be an archivist or payroll processor. It can be the case that a business is a processor in relation to the information provided to it by its customers but, in relation to its own staff data, it will be a controller.

If an employer uses a processor, for example to help with payroll, then the employer and the processor must make sure that the following is in place:

1. The processor must prove it complies with the requirements of the data protection law and must enter into a contract with the employer. Certain provisions must be in that contract including provisions protecting the rights of the staff and setting out the responsibilities on each side;Increased vigilance to ensure that employees are receiving additional contractual holiday pay; and
2. the processor must help the employer meet its data protection obligations to the staff; and
3. the processor cannot engage a further sub-processor without the consent of the employer.

Where an employer had engaged a processor before May 2018 then the employer and processor have until the end of the transition period to review their existing contractual arrangements and put in place any necessary changes to the documentation and practices. However, if the employer and processor engage in any new processing then these requirements must be met immediately for that new processing.

New right to data portability

On 25 May 2019, individuals will obtain the right to 'data portability' which allows him or her to require the controller to transfer (or copy) his or her personal data from the controller's systems and provide that data to the individual in a format that is 'machine readable' so that he or she can pass it to another organisation to go onto that organisation's IT system. This right is going to apply particularly to services such as online banking, where there is automated processing, and will help individuals transfer their information between service providers. Rarely, if ever, is it going to be a right that staff members can exercise in relation to the employer.

Action points by 25 May 2019

1. Ensure privacy notices have been provided to all staff.
2. If the business is relying on staff consent in order to process a particular type of data, consider if there is another lawful ground on which to rely. If consent is the only possibility then ensure that the consents given by staff members meet the requirements of the new law (which, an employment context, is unlikely).
3. Ensure written agreements setting out the necessary obligations of each party are signed up to with any joint controllers.
4. Complete DPIAs for use of special category data and any other DPIAs that are required by virtue of the way the employer collects and uses staff data.
5. Review and update arrangements and contracts with any processors used.
6. Review the "Transition: a plain English guide for organisations" and the technical guidance on transitional relief issued by the Data Protection Authority (www.odpa.gg)

Contacts

If you would like any further information about the above please contact us and we would be happy to help.

Louise Hall
Managing Partner
T: +44 (0)1481 748 909
E: louise.hall@walkersglobal.com

Victoria Pratt
Senior Associate
T: +44 (0)1481 748 938
E: Victoria.pratt@walkersglobal.com

Stephen Ozanne
Senior Counsel
T: +44 (0) 1481 748 913
E: stephen.ozanne@walkersglobal.com