BWCI Update on GDPR

Prepared for

Our Clients

Prepared by

BWCI Group

April 2018

Contents

1. General Data Protection Regulation (GDPR)

1.1 GDPR in the Channel Islands

Although outside the European Union, the Channel Islands will follow GDPR via equivalent local legislation. Local rules will generally mirror the EU GDPR.

The new data protection laws in Guernsey and Jersey repeal and replace the current data protection legislation in each jurisdiction. The new laws will come into effect on 25 May 2018.

The laws are enforced by the local Data Protection Office headed by an appointed Data Protection Commissioner. Data controllers (including the companies within the BWCI Group) are legally required to provide a general description of their processing and notify the Commissioner of any breaches.

The high level impact of the new laws will be to:

- Enhance the rights of individuals in relation to their personal data
- Widen the definition of personal data
- Tighten rules around obtaining consent to use personal information
- Make the appointment of a Data Protection Officer mandatory for some organisations
- Introduce data breach notification to the local data protection authority within 72 hours
- Expand liability beyond data controllers to all organisations that deal with personal data
- Introduce increased fines for noncompliance

As the new laws (and related regulations) are rolled out locally, the BWCI Group will continue to monitor the impact on our clients and on the firm. This note is intended to give a brief update on our GDPR activities. We expect to give further updates over the next few months.

1.2 BWCI Group GDPR Team

The BWCI Group has created an internal GDPR project team drawing upon resources from a variety of business areas. The team meets on a weekly basis to ensure progress towards full compliance by May 2018.

The GDPR project team has made a thorough assessment of how the new rules affect the various business activities of the BWCI Group, and has developed an overall GDPR project plan. A number of procedural changes have been identified to ensure compliance. The team is now working with the BWCI Group business areas to implement these changes and to ensure that we are able to demonstrate compliance.

1.3 Role of BWCI Group Companies

Companies within the BWCI Group may be a Data Controller (for example, where we act as Trustee to a pension or other employee benefit plan) a Joint Controller (where we perform actuarial calculations) or a Data Processor (for example, where we are administrator for an employee benefit plan or manage an insurance company). The BWCI Group companies are notified with the supervisory authorities in Guernsey and Jersey.

2. BWCI Group Actions to Date

The following sections give further details on the BWCI Group's actions to date to comply with data protection laws.

2.1 Better internal awareness of data protection and GDPR

We want all staff to be fully aware of data protection rules and general principles, and to play an active role in protecting data that we hold and process.

BWCI provides ongoing data protection training to all staff on a regular basis. Specific GDPR training will also become a routine part of induction training for new recruits and will form part of our periodic refresher training programme for established staff members. We have now given all staff training on how GDPR applies locally. In early May, we will also meet with members of staff to discuss our revised internal procedures to comply with GDPR.

Our existing Data Protection policy is being reviewed and updated as part of our GDPR project and will be supported by a number of new and updated policies, procedures and guidance.

We have asked our staff to suggest ways to enhance data security (such as making personal information anonymous).

2.2 Enhanced governance around data protection

The BWCI Group has created an internal GDPR project team drawing upon resources from a variety of business areas. The team meets on a weekly basis to ensure progress towards full compliance by May 2018.

The GDPR project team has made a thorough assessment of how the new rules affect the various business activities of the BWCI Group, and has developed an overall GDPR project plan. A number of procedural changes have been developed to demonstrate compliance with basic principles and specific rules. The team is now working with the BWCI Group business areas to implement these changes and to ensure that we are able to demonstrate compliance.

BWCI has considered a DPO. As we are not required to appoint one, we have instead chosen to appoint a Data Protection Manager to have overall responsibility for our data protection activities. The Data Protection Manager is a key member of our GDPR project team.

2.3 Legal basis for processing

We are currently documenting our legal basis for processing information. In almost all cases, the basis for our processing will fall under one of four main areas:

- It is necessary for the performance of a contract.
- We need to comply with legal obligations.
- It is in the legitimate interests of the data controller
- We have an individual's consent to process their information.

Where we rely on an individual's consent to process information, we are currently in the process of ensuring that the consent meets the parameters outlined in data protection rules.

2.4 Client Agreements

For cases where our processing is necessary for the performance of a contract with a client or Trustees, we have drafted a data protection addendum to our contracts. We are currently in the process of implementing the contract revisions.

2.5 Information for data subjects

We have developed privacy notices to inform individuals of basic details such as the information that we collect, what we do with the information, and how long we hold it. We are now in the process of distributing privacy notices where appropriate.

We are helping some clients to draft privacy notices, where needed.

2.6 Individual rights

We are developing procedures for individuals to exercise their rights under data protection rules. In particular, we will allow individuals to access the information that we hold on them under certain circumstances ("data subject access requests"). We will maintain a register of all data subject access requests.

As part of our document retention and disposal policy, we aim to hold only as much information as is needed to perform our appointed tasks and to comply with our legal obligations. Information will be deleted, destroyed, or returned to our client when we no longer have a legitimate business reason to retain it.

2.7 Transferring data to a third party

We will only share personal information outside of our firm to fulfil the terms of our client engagements. We may also be legally required to share some details (for example, to comply with tax reporting obligations). Any data transferred would be encrypted or password protected. Mail is transferred using opportunistic Transport Layer Security (TLS) which can be enforced at client request. Data transferred via physical media will be encrypted as standard. Use of Secure File Transfer Protocol (SFTP) sites to transfer data is at client request.

When transferring data to other jurisdictions, we comply with applicable data protection laws.

We will maintain a register of any third party data controllers and processors. We are currently ensuring that all will be fully compliant with GDPR and equivalent local rules.

2.8 Managing breaches

Thankfully, we have very limited historical experience with data breaches. However, we want to be fully prepared in the event that we do have a breach in the future.

Our current physical and electronic security aims to avoid breaches from happening. All staff employed by BWCI are subject to vetting. Access to the office premises is controlled by an electronic key card system. This controls the time periods and areas within the offices to which staff have access. We operate secure and controlled access to client data. Individuals only have access to the data in respect of clients on which they work. Our computer based systems contain controls and audit trails. We are implementing encryption at rest where appropriate. Websites use encryption and intrusion-prevention techniques to ensure that access is restricted to authorised users. Company laptops and mobile devices are encrypted. We monitor company email and

internet usage. We operate both clear desk and locked screen policies to limit access to information.

We are enhancing our internal procedures for reporting and logging data breaches. We are awaiting specific details on how data breaches will be reported locally.

2.9 Ongoing monitoring

We are continually improving our internal procedures, especially with respect to enhancing our physical and electronic security. Further details on security measures are given in Section 3.

We are completing Data Protection Impact Assessments (DPIAs) on internal processes where appropriate.

We will continue to monitor how we collect personal information and how the information is being used to ensure ongoing compliance with data protection rules.

3. Data Security

The following questions and answers give more details on the BWCI Group's approach to data security. We respect individual privacy and we want to do everything that we can to keep personal information safe.

3.1 Where is our data stored?

Electronic data is stored in Guernsey in the Channel Islands. Paper information may be stored in either Guernsey or Jersey.

3.2 Will our data be transferred to other locations?

We will only share personal information outside of our firm to fulfil the terms of our client engagements. We may also be legally required to share some details (for example, to comply with tax reporting obligations). Any data transferred would be encrypted or password protected. Mail is transferred using opportunistic Transport Layer Security (TLS) which can be enforced at client request. Data transferred via physical media will be encrypted as standard. Use of Secure File Transfer Protocol (SFTP) sites to transfer data is at client request.

3.3 How does GDPR affect the Channel Islands?

The Channel Islands will follow GDPR via equivalent local legislation. Local rules will mirror the EU GDPR.

The laws are enforced by the local Data Protection Office headed by an appointed Data Protection Commissioner. Data controllers (including the companies within the BWCI Group) are legally required to provide a general description of their processing and notify the Commissioner of any breaches.

3.4 How is BWCI preparing for GDPR?

The BWCI Group has created an internal GDPR project team drawing upon resources from a variety of business areas. The team meets on a weekly basis to ensure progress towards full compliance by May 2018.

The GDPR project team has made a thorough assessment of how the new rules affect the various business activities of the BWCI Group, and has developed an overall GDPR project plan. A number of procedural changes have been identified to ensure compliance. The team is now working with the BWCI Group business areas to implement these changes and to ensure that we are able to demonstrate compliance.

3.5 Has BWCI considered appointing a Data Protection Officer (DPO)?

BWCI has considered a DPO. As we are not required to appoint one, we have instead chosen to appoint a Data Protection Manager to have overall responsibility for our data protection activities. The Data Protection Manager is a key member of our GDPR project team.

3.6 What security measures are in place to protect our data?

Our internal systems are firewall protected with ongoing monitoring of attempted intrusions. We perform annual penetration tests conducted by an accredited independent tester. Remote access is limited on a business needs basis to certain employees via a secured two factor virtual private network (VPN).

All data handling and retention policies are designed to comply with statutory data protection obligations and also have regard to best business practices. We operate secure and controlled access to electronic client data whereby individual access is controlled by passwords. Individuals only have access to the data in respect of clients on which they work. All individuals are required by the system to regularly change their passwords so as to maintain appropriate security. Similarly the actions that individuals may take in relation to client data are controlled by their password level and actions are logged.

Access to the office premises (and therefore paper files) is controlled by an electronic access system. This controls the time periods and areas within the offices to which staff and visitors have access. Particular limitations apply to the data centre and related hardware rooms.

Our administrators use a fully supported third party administration system for the secure storage and maintenance of membership records. This system operates through an SQL database with the associated controls and audit trails.

Employees are contractually obligated to maintain the confidentiality of any sensitive information with sanctions for non-adherence. Third party contractors or anyone providing an in-house service to BWCI are also bound by confidentiality.

3.7 What security measures are applied in data processing?

We operate secure and controlled access to client data whereby individual access is controlled by their personal system logins. Individuals only have access to the data in respect of clients on which they work. Similarly the actions that individuals may take in relation to client data are controlled by their password level and actions are logged. We are implementing encryption at rest where appropriate.

3.8 Does the BWCI Group have a business continuity plan in place?

The BWCI Group has a full business continuity plan in conjunction with a leading computer services provider in the Channel Islands. The remote business continuity site has duplicates of the main servers used within our premises. Procedures are in place to ensure that full business continuity tests are carried out regularly.

3.9 How is data backed up?

Duplicate servers are our primary back up. Our main servers are also backed up to disk and tape each night and stored off-site.

3.10 What is BWCI's policy on data retention?

We aim to hold only as much information as is needed to perform our appointed tasks and to comply with our legal obligations. Information will be deleted, destroyed, or returned to our client when we no longer have a legitimate business reason to retain it.

3.11 How is physical data securely destroyed?

We have an onsite shredding facility for sensitive documentation. BWCI has contracted with a local business support provider to have papers records (and other media) collected in locked bins and taken to a secure facility where they are destroyed.

3.12 Does BWCI have insurance cover in place for cyber events?

BWCI has secured appropriate insurance cover against a range of cyber-related events. We can provide evidence of cover as needed.

3.13 What training does BWCI provide to staff on data protection?

BWCI provides ongoing data protection training to all staff on a regular basis. We will be training staff on the specific implications of GDPR in the period leading up to 25 May 2018. Specific GDPR training will also become a routine part of induction training for new recruits and will form part of our periodic refresher training programme for established staff members.