womblebonddickinson.com

WOMBLE BOND DICKINSON

Navigating Data Protection Liability

Key steps to help assess your data protection liability with your processors – December 2019

Navigating Data Protection Liability:

Key steps to help assess your data protection liability with your processors

Introduction

Assessing and negotiating data protection liability in contracts with your processors can often result in lengthy internal and external discussions as to what is the appropriate position. In this document we have set out a roadmap to help you get to that position.

Step 1: Identify who has responsibility for compliance with data protection law under your contract?

Statutory obligations

- Primary responsibility for compliance with the data protection principles in Article 5 of the GDPR and the DPA 2018 sits with the controller.
- Processors have their own direct obligations under the GDPR (to the extent they are subject to the GDPR). **See guidance from the ICO**[1]

Contractual obligations

How does the contract allocate responsibilities for compliance with the GDPR/DPA 2018?

Step 2: Identify any risks from a data protection perspective including any risks to the personal data

Security due diligence

What risks have been identified?

Eg risk of theft/hacking, accidental destruction/loss of access, loss of confidentiality, misuse by employees or third parties.

Due diligence on the services

- Does any part of the processing pose any risks of non-compliance with the GDPR/DPA 2018/other privacy laws? Eg any risks identified as part of a DPIA.
- Who is responsible for these areas of non-compliance (as identified under Step 1).

Personal data processed by your processor

- Does the type/volume of personal data pose an inherent risk?
- Will the processing have a material impact on the individual if something goes wrong?
- Where is the personal data held?
- Are single or multiple data sets held by the processor?
- Are multiple processors involved in the processing?
- What is the impact if the personal data becomes inaccurate, is not kept up to date or is disclosed to an unauthorised person?
- What is the impact if the processor breaches the contract or data protection law, or fails to comply with your instructions?

Commercial risk

- Is the processor reliable?
- What reputation do they have in the market?
- Where are they based?
- What is their proximity to individuals?
- What financial resources do they have and are they financially solvent?

Step 3: What are the consequences of the risks identified and possible costs/losses?

Statutory compensation claims from data subjects – Article 82(1) of the GDPR allows individuals to claim compensation from the controller or processor

Project delays and associated costs and impact on the business

Complaints from individuals and the associated costs (internal and external)

Reputational damage and adverse publicity

Loss, misuse or corruption of personal data

Regulatory action by other regulatory bodies. **See FCA fine for Tesco Bank**[2]

Ex gratia payments to customers

Damage to property eg damage to IT systems

Call centre and/or credit monitoring services costs

Legal and other advisor costs

Breach notification costs

Loss of business / revenue

Regulatory action by the ICO

Suspend data transfers outside of the EEA

Order the rectification or erasure of data

Information and assessment notices

Criminal prosecution

Penalties

- Two tiers of fines depending on which provision of the GDPR has been breached (see Article 83 of the GDPR)
- No UK GDPR fine to date, but **see notices of intent to fine BA**[3] **and Marriott**[4]
- Maximum fine for breach of PECR is £500,000

Impose restrictions/bans on processing

Warnings and reprimands

Step 4: Can you mitigate any of the risks identified?

Cyber insurance

- What does your insurance cover?
- What are the excesses, limits of cover and exclusions?
- Could it mitigate any of the potential costs identified in Step 3?

Scope

- Can you redefine the scope of the processing activities to remove/reduce the riskier data processing activities?

Data minimisation

- Does your processor need all the personal data provided for the relevant purpose?

Data retention

- Can you decrease the length of time the personal data is held?
- Processor to certify compliance
- Controller to monitor compliance and continue to review retention periods

Security due diligence

- Can any of the security risks be resolved or reduced?
- Regular auditing of processor's security measures

Accountability principle

- Ensure instructions are documented
- Ensure all the steps taken to mitigate the risks are clearly documented

Contractual terms

Include robust contract terms including as a minimum the Article 28 requirements.

- Do you want to include alternative/additional remedy obligations on your processor? Eg pro-active notification by the processor if they become aware of an identified risk, obligation to repair the data or take reasonable steps to remedy any damage/loss at own cost?
- Do you want any risks to trigger the right to suspend/terminate?

Regular auditing of a processor's compliance with the contract terms

Step 5: Choosing a data protection liability cap and approaching loss

Type of cap

- Life of contract?
- Annually re-occurring?

ICO fines

- The ICO should in principle fine the relevant parties in accordance with their degree of responsibility in the infringement (see Article 83(2)(d) of the GDPR).
- However there is no practical experience of this and this assumes both parties are within easy enforcement reach of the ICO.

Direct Losses

- Limited to types of loss, eg no loss of profit claims but will cover cost of data repair.
- Expressly include any recoverable (direct) losses.

Cap limit

- What cap(s) would you be comfortable in accepting? Tie to value of data/loss of business/ contract value?
  NB *contract value is not necessarily an indicator as to the level of risk or an apropriate metric for setting a liability cap.*
- Are there alternative remedies in addition to the cap which you would want included (as identified under Step 4)? Eg processor to provide reasonable support at own cost to fix the problem.

Scope of cap

- Separate cap for data protection liability to your processor's general liability?
- One data protection liability cap or several caps for different types of risk?
- Identify whether a risk should be under the data protection liability cap or the general liability cap.

Adjustment claims

- Article 82(5) of the GDPR provides a mechanism for claiming from the other party, a part of the compensation paid to data subjects which corresponds to the other party's responsibility in the damage.
- Untested area as to whether you can cap liability between the parties under Article 82(5). Risk that cap may therefore be unenforceable.
- Possible options in relation to a processor's liability to a controller include: (a) an express statement that this type of liability is uncapped; or (b) if drafting is ambigious, accept risk that it is not clear whether the cap covers this type of liability or not, and if so, acknowledge risk as to the cap's enforceability.
- Depending on the approach taken, a processor may ask for a reciprocal approach eg that the controller's liability is also uncapped.

Authors

Amy Eames
Associate
T: +44 (0)238 020 8379
E: amy.eames@wbd-uk.com

Katie Simmonds
Associate
T: +44 (0)207 788 2415
E: katie.simmonds@wbd-uk.com

Andrew Parsons
Partner
T: +44 (0)2380 20 8115
E: andrew.parsons@wbd-uk.com

Peter Given
Legal Director
T: +44 (0)238 020 8194
E: peter.given@wbd-uk.com

Hyperlinks

1. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-a-processor/#1
2. https://www.womblebonddickinson.com/uk/insights/articles-and-briefings/tesco-banks-cyber-attack-series-unfortunate-events
3. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/
4. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/