DIXON WILSON
CHARTERED ACCOUNTANTS

# GDPR – Our Approach

1 March 2018

## INTRODUCTION

This note sets out the initial steps Dixon Wilson is taking to ensure the firm complies with General Data Protection Regulation (GDPR). We expect this note to be updated as it becomes clearer how GDPR should be applied in practice.

## DATA AUDIT

The GDPR requires all businesses to demonstrate they are processing data legally and protecting the rights of individuals regarding the personal data held.

Understanding what data the firm holds and uses across the business will help the firm comply with the new regulations. For this reason, a full data audit is being carried out internally. As part of this audit, we are in the process of:

1. Identifying the personal and sensitive data the firm holds.
2. Documenting where the data is stored, how the data is used and with whom the data is shared.
3. Establishing from where the data came from and identifying the legal basis for holding and processing it.
4. Determining whether the data has been stored outside the firm's agreed retention period and considering whether we need to continue to hold that data.

## SECURITY REVIEW

We are reviewing relevant security measures to ensure systems are robust and personal data is safeguarded. This will help the firm identify any potential risks of non-compliance or any weaknesses in our data storage and handling systems.

### CYBER ESSENTIALS CERTIFICATION AND ISO 27001

We have continued to upgrade cyber security systems over the last few years irrespective of GDPR. The firm is considering certifying to the Governments Cyber Essentials Scheme and implementing ISO 27001.

The Cyber Essentials Scheme is a government-backed scheme to help organisations protect themselves against common cyber attacks. In order to obtain accreditation, businesses need to contact one of the relevant certification bodies and carry out an assessment.

The ISO 27001 provides a starting point for achieving the technical and operational requirements necessary to prevent a data breach under GDPR. This requires an independent review of company procedures before certification is given.

Dixon Wilson will be using a consultant to help achieve the necessary accreditation.

### DATA ENCRYPTION

As a minimum, Dixon Wilson expect to be sending personal data by encrypted attachment, and we are seriously examining how best to achieve fully encrypted communication with clients practicably. We will then implement the appropriate procedure ahead of May 2018.

## SUPPLIER REVIEW

Dixon Wilson will be engaging extensively with the handful of organisations with which we share data.

All businesses where data is held in the cloud should check that the provider is compliant with GDPR.

We will also be identifying any arrangements where it will be necessary to have data sharing agreements and contracts in place with third party processors which set out respective responsibilities under GDPR.

## DATA PROTECTION OFFICER

Dixon Wilson is not required to have a Data Protection Officer (DPO). However, we intend to appoint a senior member of staff as "Head of Data Privacy". This is to increase the status attached to and priority given by staff to data protection within Dixon Wilson.

## REPORTING A DATA BREACH

We will have clear policies in place for reporting a data breach. We are doing this not simply so the firm can notify the ICO (Information Commissioners Office) but also anyone (including employees and clients) whose data may have been compromised. Our instructions to employees are that if any employee becomes aware of a data breach, it should be reported to the DPO immediately.

DIXON WILSON
CHARTERED ACCOUNTANTS

## LEGAL BASIS FOR PROCESSING DATA

It is important that all businesses identify the legal basis for processioning data and document it. We are considering the most appropriate way to achieve this - either by consent or as required for performance of a contract.

We anticipate that a new engagement letter or an addendum to our existing letter will need to be issued to all clients ahead of the GDPR enforcement date.

## PRIVACY NOTICES

Data controllers are required to continue to provide transparent information to data subjects. The firm will be reviewing privacy notices to ensure they are in line with GDPR and are in clear and plain language.

The information to be provided must be more comprehensible and inform the data subject of their rights and the period for which data will be stored.

## PRIVACY BY DESIGN

We intend to ensure that privacy is considered when implementing any new product or service. We will endeavour to bring this into all projects we contemplate early in the process and not as an afterthought so as to ensure and be able to demonstrate compliance with the GDPR.

## DATA SUBJECT RIGHTS

We will ensure that procedures are in place to deal with individual's enhanced rights under GDPR, such as the right to data portability and the right to erasure.

Data subjects now have the right to have data transferred to a third party service provider in machine readable format and we are implementing policies to facilitate this.

## STAFF TRAINING

All employees are being made aware of the new data protection regulations and the implications of non-compliance.



Dixon Wilson
22 Chancery Lane
London
WC2A 1LS

T: +44 (0)20 7680 8100
F: +44 (0)20 7680 8101
DX: 51 LDE

www.dixonwilson.com
dw@dixonwilson.co.uk