HYMANS ROBERTSON

How Hymans Robertson has risen to the GDPR challenge

We take data seriously. In many ways, it's the life-blood of our business. That's why we set ourselves the challenge of becoming compliant with the General Data Protection Regulation (GDPR) well before its 25 May 2018 effective date.
Now that deadline is upon us, how have we done?

Conforming to the GDPR has been our highest-priority internal project for well over a year. We approached the task in a structured manner, establishing a steering group with executive-board sponsorship, and five work streams responsible for particular aspects of our preparations. Their tasks were to:

- Review, document and improve our data-handling activities;
- Review our technological and organisational measures for ensuring data security;
- Refresh our data protection policies and information governance arrangements;
- Engage and communicate with clients;
- Train our people on GDPR and foster a culture of data privacy within our firm.

Over the next two pages, we summarise the most important outcomes of the project.

Message from James Entwisle, Managing Partner

Our aim is that our clients should have absolute confidence in the way we protect the data that you entrust to us. As such we've invested heavily in processes, technology, and above all in our people so that we are a centre of excellence in data protection.

Over the last 18 months or so, we've taken the ISO27001 Information Security standard that we have held for many years as a solid foundation. From there we have enhanced our internal policies, processes and systems. We have scrutinised – and tightened-up where necessary – the way in which we receive, hold and share data internally and externally.

We've trained our people wherever necessary so that we have data protection designed into all that we do. We've also been working with you, our clients, with the same goal.

We know that we'll need to keep learning and developing our compliance framework in this ever changing world. This document recognises the hard work of our people so far, and our commitment to continued evolution of our approach, so that you can be assured of our high standards in this vital area.

Privacy by design and by default

- We have updated our data collection templates, specifications and processes to help ensure that the data that we process for you is minimised.
- We know that in some cases it will take time to adapt to these changes: we will continue to work with you and other external parties through this transitional period.
- We have a Data Protection Impact Assessments (DPIA) policy and guidance in place, and a process to support DPIAs for new and changed uses of personal data.

Security of personal data

- Hymans Robertson is ISO27001:2013 and Cyber Essentials certified.
- We have reviewed our controls and implemented some new measures to protect personal data.
- For example we have implemented a sophisticated Data Loss Prevention solution, which mitigates risk of data leakage by email and have introduced ShareFile for securely sharing bulk personal data.
- We have made changes to focalPOINT (our secure document and meeting management tool), to give you more control over security.

Data retention

- We have refreshed our data retention policy.
- In general, we will archive data after 7 years and delete it after 20 years.
- Different rules apply for our third-party administration practice.
- Please speak to your Hymans contact for a copy of our "Working together under the General Data Protection Regulation" communication for more details.

Breaches

- We require all staff to report actual or suspected personal data breaches, and provide them with an easy and speedy way to do so.
- We have rolled out specific breach training to our practice representatives, who are cascading this in their teams.
- We have a Data Breach Response Plan in place to deal with a serious breach.
- We will notify you of any breaches in accordance with GDPR rules and timescales and our contractual commitments to you.

Accountability

- We appointed a Data Protection Officer (DPO), with effect from 1 December 2017.
- We have refreshed our data protection policies.
- We have mapped our data flows and documented our data processing activities and will continue to update and maintain these records.
- We are assembling all of our compliance materials into a central Privacy Hub.

Individual rights

- We have published a new individual rights policy, supported with guidance, and a mechanism to report any requests received by you and by our DPO.
- We will handle all individual rights requests in consultation with you and in accordance with GDPR rules and timescales and our contractual commitments to you.

Our people and culture

- Our senior staff are responsible for fostering a culture of data privacy in the firm.
- Everyone in the firm is committed to confidentiality and required to handle personal data in compliance with data protection laws.
- We have run "train the trainer" sessions for 80 data protection representatives from around the firm, who are responsible for cascading information in their teams.
- We have updated our mandatory training module, and require all staff to complete this during June 2018 (and annually thereafter).
- We have launched a Privacy Hub for staff, bringing together all of our training materials, policies and a wiki-style guide to data protection fundamentals; thus allowing them to easily initiate a data protection impact assessment, record data subjects' requests to exercise their rights, or report a personal data breach.

Third parties

- We have refreshed the due-diligence checks on all suppliers who process personal data for us.
- We have issued updated contractual terms, mirroring those that we have agreed with you, to all of our suppliers.
- We have published a list of our sub-processors in our online Trust Centre www.hymans.co.uk/information/trust-centre.

Our legal agreements with you

- We have issued GDPR-compliant contractual terms to all of our clients, for whom we process any personal data.
- Where applicable, included in those terms is a document setting out the allocation of responsibilities between you, us and the scheme actuary (if there is one) as joint controllers.

Keeping you informed

- We have prepared monthly GDPR project updates since June 2017.
- We have produced Sixty Second Summaries of important data-protection issues.
- And this brochure!
- We have created an online Trust Centre www.hymans.co.uk/information/trust-centre, as a hub for data protection and information security matters.
- Our Trust Centre contains our privacy and cookies policies, details of our ISO 27001 certification, details of how we process our clients' pension schemes' member data, downloadable copies of our data-protection Sixty Second Summaries, and a list of our sub-processors.

Message from Brian Taylor, Data Protection Officer

Very early on in our GDPR project, I recorded a short video for our people, highlighting the importance of the two main themes of GDPR: transparency and accountability.

Transparency means that we all need to be clearer about what data we have and how it's used, and accountability means we need to be able to demonstrate how compliance with data privacy laws is embedded in our organisation and is part of our culture.

Our data protection compliance framework – summarised for you in this document – means that we can deliver on this.

But the job is ongoing. My role is to help our senior management team ensure that these themes remain at the heart of what we do, as we move from project delivery to business-as-usual and ongoing assurance.

Your usual Hymans Robertson contact will remain your go-to person in the event of any queries you have about data privacy. However I will be only too pleased to help where I can.

You can contact me on **0131 656 5167** or at **dataprotection@hymans.co.uk**

Brian was appointed as the firm's Data Protection Officer from 1 December 2017, reporting to the Board Executive. He is a practising lawyer and certified data protection practitioner and has been closely involved with Hymans Robertson's GDPR project since the outset.

Time to acclimatise

Of course we, like everyone else, are getting used to the 'new normal': it will take time for the GDPR to become embedded in our business. We will review and critically assess our performance over the coming months. In parallel, we'll support our clients as they adapt to our new processes, data requirements, etc.

'It's an evolutionary process for organisations: 25 May is the date the legislation takes effect but no business stands still. You will be expected to continue to identify and address emerging privacy and security risks in the weeks, months and years beyond May 2018.'[1]

UK's Information Commissioner, Elizabeth Denham

[1] Extracted from ‹https://iconewsblog.org.uk/2017/12/22/gdpr-is-not-y2k›.

Call to action

Your Hymans Robertson contact will work with you to:

- Discuss ways of minimising data that is sent to us by you or on your behalf.
- Include information about Hymans Robertson's use of personal data in your privacy notice.
- If we provide administration services to you please share your privacy notices with us so that we may discuss implementing these into our processes.
- Get GDPR-compliant contract terms in place. If you have not signed and returned the terms issued, we will assume these apply from 25 May 2018 unless you tell us otherwise.

Please also make sure that we have a note of the contact details for your Data Protection Officer or other person responsible for data-protection matters, and who we should contact in an emergency.

- Finally, review the materials on our online Trust Centre www.hymans.co.uk/information/trust-centre, including our list of sub-processors.