

## COMPASS GROUP, UK AND IRELAND LIMITED

### GDPR COMPLIANCE PROJECT: POSITION STATEMENT

In response to your communication in relation to Compass's compliance with GDPR, we confirm that Compass has been pursuing a detailed compliance programme which is now entering the remediation stage for such GDPR failures as have been identified.

Notwithstanding the nature of your enquiry, as a large business with thousands of suppliers and customers, we are receiving a substantial amount of similar enquiries.

These range from simple letters asking for our position, to detailed and complex surveys and questionnaires, completion of which would demand an extensive amount of resource; which we should prefer to dedicate to the compliance programme itself.

Accordingly, in response to your enquiry, we have developed the following position statement to illustrate how our compliance programme is progressing.

We have approached the issue of GDPR compliance with a three-phase plan:

**Phase 1** was to undertake a survey, across all business sectors and central functions, to identify what personal data was being processed, where it is stored, on what systems and for what operational reasons; with the survey also confirming whether any data was exported to or otherwise processed outside the EEA.

This analysis focused on what third party personal data or employee data we process ourselves and what personal data of ours, particularly our own employees' personal data, is processed by our own processors (or sub-processors).

**Phase 2** analysed the output from Phase 1 and identified the type of personal data being processed (personal data, special category data or criminal data) and also the legal justification for the processing (statutory, contractual, consent or other legitimate reason). Again, this was across all business sectors and central functions.

With this phase having been completed, it indicates that few elements of the personal data processed by Compass require consent and that the vast majority of personal data processed by Compass is processed for a contractual or statutory justification.

Phase 2 also identified whether the processing identified was GDPR compliant or whether it amounted to a failure to meet that standard. The most common failure was a failure to meet data retention and/or data security policy expectations.

For example; keeping multiple copies of the same document, keeping documentation for too long, keeping documentation on shared computer drives with insufficient access control, or keeping hard copy documentation in filing systems whose security could not definitively be confirmed.

Compass is re-issuing its Data Retention Policy for 25 May 2018 and issuing a new Data Security and Incident Reporting Policy at the same time.

There were very few exceptional data protection failures that indicated a major risk. As above, most were identified as operational data management having become less rigorous than is ideal with the major “consent” issue being limited to those business sectors who do have an element of B2C business.

**Phase 3** is the remediation phase. It seeks to plan, across Compass business sectors and central functions, how the identified heads of failure will be corrected.

Remediation for the majority of the data management failures identified will be to ensure that the Data Retention and Data Security and Incident Reporting policies are enforced by local management throughout Compass’s operations.

Compass is reviewing all documentation and policies impacted by GDPR and the new documentation will comply with the GDPR. Internal guidance on measures to follow to ensure our operations are practically managed in line with GDPR expectations will be in place by 25 May 2018.

In reality, the cascading of best practice reminders has already started, following the individual business sector and central function analyses that have taken place, such that the vast majority of remediations across Compass’s whole business will be complete by 25 May 2018.

**As at 9 May 2018**