thorpemolloy Recruitment

General Data Protection Regulation (GDPR) Policy

General Data Protection Regulations (GDPR)

The General Data Protection Regulations (GDPR) is a piece of human rights legislation aimed at placing power back into the hands of the individual with respect to how their personal data is used. In 2016 surveys showed that more than 97 per cent of the British population had concerns about sharing personal information with under 15 per cent believing they were in control of their personal information. GDPR and the subsequent UK Data Protection Bill is a piece of legislation aimed at tackling this level of distrust.

Many of the GDPR's main concepts and principles remain much the same as those outlined in the Data Protection Act (DPA) of 1998 and, whilst complying properly with that law, we recognised that GDPR placed a greater emphasis on the documentation that data controllers such as recruitment agencies must keep in order to demonstrate their accountability. Compliance with all the areas listed in this document has ensured we have accordingly reviewed our approach to governance and illustrates how we manage data protection as a corporate issue.

Awareness and Training

The actions taken prior to the GDPR implementation date included:

1. We made sure that all staff in our organisation were aware that the law was changing and ensured that staff fully appreciated the impact this was likely to have.

2. Areas that could cause compliance problems within the recruitment sector were identified.

3. Internal training and a subsequent assessment of staff competence and knowledge levels was successfully conducted across the workforce in April 2018.

Data Protection Officer (DPO)

We are not required to appoint a DPO on the basis we are not involved in the regular and systematic monitoring of data subjects on a large scale, we have chosen to appoint a designated Head of Data Protection who will take responsibility for our data protection compliance. This role will be undertaken by Steve McCulloch, our Associate Director. Steve has over 16 years direct experience of the recruitment industry and our business but his current role also sits autonomously within our structure and is therefore without conflict to the core function of the business. Steve also has direct access to board level communications therefore is able to influence change with respect to Data Processing best practice. In appointing this role, we feel we have someone who will take responsibility for our data protection compliance and has the knowledge, support and authority to do so effectively.

Updating Client Contracts

We updated our Terms of Business and all candidate and client paperwork to reflect the new law. We have worked closely with our clients to reflect the new legislation within all of our existing and future contracts and to define our respective obligations.

Introducing A Better Consent Process

Whilst we never used to imply 'consent' to data sharing by using pre-ticked boxes the new rules have recognised the importance of consent being a definite, obvious 'yes' by the individual. We have therefore improved our processes to make it easier for clients, candidates and new contacts to actively 'opt in' for business activities such as sharing feedback on our service.

Information We Hold

Through organising an information audit, we have documented the personal data we hold across our business, where it comes from and who we share it with. This has helped us to comply with the GDPR's accountability principle, which requires we are able to show how we comply with the data protection principles e.g. we have effective policies and procedures in place. A process is in place to ensure that this data is regularly reviewed so that it remains accurate and up-to-date.

Communication of Privacy Information

Recognising the importance of communicating updates and changes in light of the new Data Protection Laws, we reviewed and updated our data privacy policy accordingly: www.thorpemolloy.com/privacy.php

Our enhanced privacy policy has been shared with the candidates we are currently representing and is clear, concise and jargon-free. The content of the policy explains the information we need to fulfil our obligations and how we will process data under the legal basis of legitimate interest.

Individual Rights

On the whole, the rights an individual enjoys under GDPR are the same as those under the DPA but with some significant enhancements.

We have procedures in place to fully recognise their right to:

- have information erased;
- make a Subject Access Request (SAR);
- have inaccuracies corrected;
- data portability;
- prevent direct marketing; and
- prevent automated decision-making and profiling.

Subject Access Requests (SAR's)

We are conscious we could experience an increase in the number of SAR's and our revised procedures ensure any such requests can be handled within the new timescales. We did not charge an individual for complying with a request under the DPA and have had no past problems in providing the necessary information within 30 days therefore feel prepared for this element of the new legislation.

Our Data Retention Policy

It's in everybody's interest to make sure retained data is accurate and relevant. We have taken this opportunity to streamline the process for candidates to gain access to their personal data, as well as to outline clear procedures to meet regulatory and legal requirements:

Our data retention policy in summary is as follows:

- We will only keep data on candidates that is relevant to our business relationship e.g. contact details and a current CV.
- If a candidate has been paid by our payroll services, we will keep relevant data for HMRC purposes for as long as is necessary.
- Generally though, if we have had no meaningful contact with a candidate for 5 years, we will delete all their personal data.
- At any time, a candidate may request that we delete their personal information. The candidate will be informed of what deletion means for them and their relationship with Thorpe Molloy, and what personal data can be deleted within 30 days of their request.

Data Breaches and Reducing Their Likelihood

Acknowledging that the GDPR has introduced a breach notification duty across the board, we have procedures in place to detect, report and investigate a personal data breach. This was achieved by assessing the types of data we hold and documenting those which fall within the notification requirement should there ever be a breach where the individual is likely to suffer some form of damage, such as through identity theft or a confidentiality breach. All our staff will continue to receive regular, on-going communications and education on how to minimise the risk of a personal data breach, and who to inform if a breach occurs.

We now work on a privacy by design approach across all projects, in order to:

- Promote privacy and compliance from the start of every initiative;
- Reduce operational risk, and ensure that all initiatives are risk-assessed on data privacy needs.

We will continue to make sure user passwords are secure, data visibility is controlled by seniority and financial data is made very difficult for unauthorised people to access.

Do you need further information?

If you have questions or need further information about our approach to GDPR, please contact us on DataProtection@thorpemolloy.com and we will be happy to discuss any specific questions you may have.

thorpemolloy
Recruitment

38 Albyn Place, Aberdeen, AB10 1YN
T 01224 658 865 **E** hello@thorpemolloy.com www.thorpemolloy.com

Registered in Scotland No. 176282