HRC Law TEAM GD:PR

Be prepared for GDPR: checklist

We have training in place for:	
Business decision makers on what GDPR means	
Employees and other staff on what GDPR means	
Both of the above, re actions needed, and to ensure awareness on an ongoing basis	
Audit & key analysis. We have, or have plans in place to:	
Review our **current data** so that we know: • What data we hold; • Where it came from; and • On what legal basis that data is processed.	
Understand **data movement**, including: • Where data comes from and to where it is transferred (geographic); • Who are the senders and recipients (from and to whom); and • Whether the data enters the public domain.	
Understand **consent** (of the data subject) including: • Are we relying on consent for processing? • How consent was/is obtained; and • What information was/is provided at this time.	
Understand any other (policy, legal or practical) **restrictions** on processing data, including: • How long the data is kept for; • Whether the data can be deleted; • How the data is kept secure; and • Whether the data is pseudonymised.	

Acceptability & Record Keeping. We have, or intend to put, the following records in place:	
Records of the legal basis for processing data. (We have established a record of our current processing on a "who, what, where, when" basis.)	
Record of Management/the Board's decisions. (We have created a register for these).	
Log of Data Subject Access Requests (**DSAR**s).	
Log of consents (including e.g. duration of, and any other restrictions on permission).	
Record of data breaches.	
Document Review. We have reviewed, or have prepared, the following documents	
Terms of business and terms of engagement.	
Privacy Notices (including when data received from third party).	
Website terms.	
DSAR response format	
Document Retention Policy	
Employee Handbook	
IT Policy	
Data Protection Policy	
Response processes. We have processes in place to deal with:	
Data portability.	
Responses to rights enforcement.	
Deletion of data.	
DSARs.	
Data breaches and allegations of such.	
Communicating with the data recipient.	
Integrated processes. We understand the need for and have processes and documents in place regarding:	
Privacy by design and default (criteria and policy).	

Data Protection Impact Assessments (format and content).	
If applicable, built-in processes for verifying age of data subject.	
Organisational Technology Measures. We have (and can show that we have):	
Appropriate organisation and security measures in place.	
Considered pseudonymised data (particularly where this would benefit the data subjects and/or the business).	
Considered the creation of a running log recording the basis and duration of processing.	
Contracts. We understand our roles and obligations and the other party's/parties' roles and obligations under contracts to which we are a party. Where applicable, we have:	
Reviewed contracts with processors (i.e. where we are data controller) e.g. those with subcontractors.	
Reviewed contracts where we will be processor (and another party will be data controller).	
Where applicable, reviewed/created a Joint Controller arrangement (is a contract appropriate?).	
Established with whom we are contractually jointly and severally liable and what the limits of our liability are (if any).	
Reviewed our Employment Contracts and obtained consents where required.	
Supervising Authority. We have:	
Determined who our SA will be (it is likely to be the ICO).	
Data Protection Officer. We have considered:	
Whether we need one.	
If we do need one, who it will be and where they will they sit within the business.	
If we do need one, how we will ensure their independence and involvement in governance.	
If we don't need a DPO, we have identified an individual responsible for GDPR compliance	

HRC Law would be happy to assist you or your business with any GDPR issues. Graham Hansen, Associate at HRC Law, can be contacted on 0161 358 0552 or at grahamhansen@hrclaw.co.uk. You can find out more about Graham and HRC Law at www.hrclaw.co.uk.