Adapt Consulting Company Limited

Task: Support Small Businesses with guidance and tools for GDPR.

ROLE: My role as consultant was to advise, guide and support necessary changes for the organisation to be ready for and compliant with the new GDPR regulations.

ISSUES: General Data Protection Regulation [GDPR)} affects all organisations holding personal data. is a need to develop the policies, procedures and guidelines to ensure that people, process and technology all work together to keep personal data private, safe and secure.

ACTION: Set-up a series of meetings to understand the business and support necessary actions to achieve GDPR compliance. Key Elements [1] Education and Awareness [2] Data Mapping [3] A Records Management & Retention Policy [4] Risk Assessment [5] Subject access request [6] Data beaches and reporting [7] A Data Protection Policy [8] An Information Security Policy [9] Processor/Controller Agreements [10] A Privacy Notice

OUTCOME: A series of tools, templates, training and guidance to safeguard data and help ensure compliance with the law.

TESTIMONY:

I think yesterday went very well – in fact I think it is the best £70 we have spent for a while. The reason I say this is because you have given us some very practical pointers which we feel is relevant to our business – others have simply bamboozled us with high tech tools and tried to scare us into purchasing them

Truusje Gamlin - Hollcameron

From the outset Tim's style, manner and pragmatic approach distinguished him from other consultants. For one, he was deeply knowledgeable and enthusiastic about the topic and we had a real sense of being supported by someone with a clear focus on achieving our objectives. Tim was happy to adopt our chosen preference for one to one engagement and desire to address the detail of the practical implications. He was able to distil complex matters into readily understandable actions. Our lasting impression of Tim's work with us is one of ease of communication, total commitment and a reassuring knowledge of the subject matter.

Stephen Eldred CommunitySavings

Adapt Consulting Company

BREAKDOWN OF DELIVERABLES

Education and Awareness – Use posters, team huddles, reminders and staff handbook to remind people about their obligations (eg the stuff in your Data Protection Policy and Information Security Policy).

Data Mapping (Understanding what data you hold, where and why) This is good to help identify "trip hazards" that need addressing around people, process or technology, making sure there are roles and controls to keep data private, safe and secure.

A Records Management & Retention Policy To help you to classify/categorise data and treat it accordingly with some being held for 1 year, 3 years, 10 years (or what-ever) and some being restricted to authorised people only. Generally this is also a good housekeeping exercise.

Risk Assessment (Understanding and agreeing key risks and measures over people, process and technology). There is a lot you could do on risk and there is some guidance on data-processing impact assessments [DPIA]. As a minimum I'd suggest that your Directors (or Audit) have a meeting to discuss training, measures and paperwork and the minutes of that meeting (together with any actions) can constitute a reasonable risk assessment.

Subject access request - Have a standard process and perhaps template response for dealing with requests which may be from staff, customers or other "types" of people for whom you hold or share data.

Data beaches and reporting – Have a standard process and perhaps template response for dealing with Data beaches and reporting, include any that are as a consequence of a supplier, third-party or any other person holding your data.

A Data Protection Policy (About data, confidentiality, security, privacy etc) You probably already have this covered in your staff handbook

An Information Security Policy (About emails, login, passwords, clear desk-policy, cabinets and keys) You probably already have this covered in your staff handbook too

Processor/Controller Agreements – Have a standard letter to send to supplier, third-party or any other person holding, sharing or processing your data. Make sure that letter (or contract) sets out your expectations and their obligations (eg the stuff in your Data Protection Policy and Information Security Policy – see above)

A Privacy Notice (About what data you hold, why and key controls taken to keep confidential, accurate and secure). Some of this may be on your website, some may be written into your contracts, or possibly on a leaflet or brochures.