General Data Protection Regulations (GDPR) Checklist

We recommend you watch the Video Masterclass or have a read oft he information on the webpage explaining GDPR and its requirements before you go through this checklist. It’s worth re-iterating here though that GDPR is not the onerous regulation that grinds business to a halt that some claimed it to be when it was first introduced. Think about it as all about handling your customer’s data as carefully as you’d like your own data to be handled, then it can really help businesses bring in some best practice around operational principles and practices. The check list below is designed to help ensure you follow the logical steps needed to protect the data you hold.



|  |  |
| --- | --- |
| Action | Check |
| 1. Nominate someone in your business (it could be you) to be responsible for managing and monitoring all aspects related to GDPR. This doesn’t have to be a specific role dedicated to GDPR (unless you are an organisation that requires this) – but rather incorporate responsibilities into a current role |  |
| 2. Assess specifically what data you ask for and hold for the following groups of people: - 1. Potential customers
2. Customers
3. Potential employees
4. Employees
5. Potential suppliers
6. Suppliers
 |  |
| 3. For each piece of information that you hold on each of the above data subjects, list out why you need each element of the data1. For contractual reasons (to deliver a product/service)
2. For practical reasons (to pay someone)
3. For legal reasons (to comply with HMRC etc)
4. For other specific and explicit purposes
 |  |
| 4. For each piece of data that you hold, have you obtained specific permission to hold this? Do you have an opt in record? |  |
| 5. For each piece of data that you hold, where is this stored? |  |
| 6. For each piece of data that you hold, who has access to it? |  |
| 7. For each piece of data that you hold, if the data will subsequently be processed by a third party, do you have a written contract that specifically states how the data will be securely shared, processed, deleted? |  |
| 8. For each piece of data that you hold, how long is it necessary for you to hold the data for? |  |
| 9. For each piece of data that you hold, how will you securely delete it? |  |
| 10. How have you notified each data subject about your data capture, processing, management and retention policy? |  |
| 11. Delete any records/data that does not comply with the regulations. |  |
| 12. Based on your above audit, create a policy that clearly describes what data you hold for each data subject type; why you need to hold the data; who you share it with; how long you hold it for; how you look after the data (i.e. where you store it); how someone can contact you about the data you hold. 1. This policy should be available on all your external marketing materials and communication
2. The policy should also form part of your employee handbook
 |  |
| 13. Ensure that your IT system (including networks and routers) is securely protected with firewalls, anti-virus software, guest Wi-Fi. |  |
| 14. Ensure that all staff are trained on the ethos behind GDPR, your specific policy and all procedures that are in place to ensure the policy is adhered to. |  |
| 15. Create an audit schedule whereby you can check the effectiveness of your policy and improve as necessary. |  |
| 16. Create a GDPR training schedule so that staff are at least annually reminded of their responsibilities and your responsibility as an employer. |  |
| 17. Ensure you keep detailed records of all your actions in relation to GDPR. |  |

