

Virtualgo2 - Compliance and Tech Starter Checklist

The following are key areas for your business to set it up for data protection compliance and safer app, platform, software, and device use. The list does not cover every single item in depth but it will give you a starting point.

Item	Subject	Notes
<i>Training - start at the beginning</i>	GDPR requires data protection training (annually is usually sufficient). It will help you to identify the basics for your business and make your responsibilities easier to follow.	I have a Basics of GDPR Online Course which takes a total of 1.5 hours with a certificate for your records. A useful resource with 12-month's access and updates. There is a discount for Grow Her Business members.
<i>Know your Role(s) & Responsibilities</i>	You will be likely a Data Controller for some activities & a Data Processor for others. You need to know the role you fit for each purpose for which you process personal data.	A Data Controller is responsible to the people whose data is processed and carries the full responsibility for this. A Data Processor is responsible to the DC & follows their instructions.
<i>Register with the ICO (UK Data Protection Authority)</i>	UK-based organisations are required to register with the Information Commissioner's Office. There is a fine for failing to do so & an online searchable list of those who are caught.	There is an interactive assessment to see if and how much you should pay. https://ico.org.uk/for-organisations/data-protection-fee/register/
<i>Know what you use</i>	A simple list of the digital tools & devices you use will make your compliance easier.	Include useful information & update the list as you go e.g. location of their servers (for the USA, if they are Data Protection Framework registered)
<i>Record the where and why</i>	A second list of where & why you collect personal data	Include the Lawful Basis you have chosen as most appropriate. This list will also help you fulfill Data Subject Access Requests.
<i>Keep people informed</i>	Your public-facing documents must be accurate, understandable & explain how and why you process personal data, amongst other things.	Your Privacy Notice(s) are the most well-known. Your website should have a Cookies Policy and Cookie Control Banner to obtain consent.
<i>Safer marketing</i>	The biggest area of misunderstanding & risk. You must have consent (& a record of what, when & who gave it) for electronic marketing.	A soft opt-in is allowed when: the person has been in direct contact with your business, you have obtained their details directly from them, you are marketing a similar product (they will be interested) & they can opt out from future marketing easily (unsubscribe).
<i>Policies</i>	Write down why (policy) and how (procedure) you do things in your business to ensure consistency.	Share your policy document with employees or contractors as you grow.
<i>Tech matters</i>	USE: Strong passwords, a password manager, MFA, recovery options & security checks, and always choose secure (& encrypted) apps, platforms & services.	Set up & keep your devices (laptop, smartphone, tablet, etc.) secure physically & digitally. Activate "find my device" & remote wipe wherever possible.
<i>Get help!</i>	GENERAL: Contact me in the GHB Community. Connect with me on LinkedIn. Check out my website & blog for more information.	SPECIFIC & IN-DEPTH: Book a free Introductory call & we can find the answer that works for you.
<i>Additional useful URLs to help you</i>	ICO Direct Marketing Advice Generator: https://ico.org.uk/for-organisations/advice-for-small-organisations/checklists/direct-marketing-advice-generator/	
	ICO Direct Marketing Checklist: https://ico.org.uk/media/for-organisations/documents/1551/direct-marketing-checklist.pdf	