

# GDPR Compliance Checklist for SMEs



## Have you done a GDPR audit to identify:

- The type of personal data you've collected or stored.
- Whether you've collected this data fairly.
- Whether you got the necessary consent from data subjects.
- Whether you clearly told data subjects why you're collecting data.
- Whether you told data subjects that they can withdraw consent at any time.
- Whether you've made sure you're not holding info for longer than necessary.
- Whether all the data you hold is up-to-date and accurate.
- Whether you hold data in a safe and secure environment.
- Whether you are using the data for its intended purpose only.
- Whether you've collected or processed any special categories of personal data and if you are meeting the standards to collect, process and store it.
- Whether you know or have documented the source of any personal data.
- Whether you are sharing any personal data.

## Have you put a GDPR Project Plan in place to make sure you're compliant?

### Your plan should identify:

- If you need a Data Privacy Impact Assessment.
- If you need to hire a Data Privacy Officer.
- If you need to implement a policy of 'Data Protection by Design and Default'.

## Do you have GDPR compliant procedures to handle requests from data subjects to amend, delete or access their personal data?

## Do your GDPR compliant procedures make sure that you handle data requests in a timely manner?

## Do you have a process in place to spot, investigate and report personal data breaches?

## Do you have a security notification procedure in place on how to deal with a data breach quickly?

**Are you planning to hold ongoing and regular reviews and audits of the data you hold?**

**Have you updated your privacy policy to cover the new rights of individuals?**

**Do you have a system in place to show how you comply with the data protection principles?**

**Do you document all internal procedures?**

**Have you informed external parties when you've received inaccurate personal data?**

**Have you updated all third party contracts to be GDPR compliant?**

**To make sure you get consent in a free, specific, informed and clear way, have you reviewed how you:**

- Seek consent from a data subject?
- Get consent from a data subject?
- Record consent from a data subject?

**Do you record data consent and can you demonstrate that you've received it?**

**Do you have a process in place to verify someone's age and get parental or guardian consent when processing children's data?**

**If you operate internationally, have you decided which data protection supervisory authority will be the lead for the business?**

**Have you given GDPR training to your staff? If so, do they understand:**

- The difference between Data Protection Act (DPA) and GDPR?
- Their responsibilities under GDPR and what day-to-day processes need to change?

If you have any questions about GDPR compliance for your business, call our brilliant BrightAdvice team today on **0800 783 2806**.



\*Source of information: ICO (Information Commissioner's Office)

Bright HR Limited, The Peninsula, Victoria Place, Manchester, M4 4FB