GDPR Outsourcing Partner Compliance Checklist

If your business works with clients in the UK or Europe and you outsource you need to make sure your partner is GDPR compliant.

This checklist will help you determine if you're at risk and how compliant your offshore partner is.

1. Have they been audited and certified by an external body? ☐ YES ☐ NO

Anyone can claim to be GDPR compliant but to actually be compliant, their systems and processes need to pass through stringent auditing by an independent certification body. By being BS 100012 certified by a standards body such as the British Standards Institution (BSI) it demonstrates that the offshore partner can manage risks to personal information.

Certifying to BS 10012 Personal Information Management means your offshore partner upholds the ideologies of the GDPR and provides reassurance that personal data is managed in line with best practices. A compliant offshore partner will establish a Personal Information Management System (PIMS) so that personal data is managed in line with GDPR best practices. Your outsourcing partner needs to establish, implement, maintain and continually improve the PIMS.

2. Do they have a qualified and certified data protection officer? ☐ YES ☐ NO

DPOs assist in monitoring internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and operate as a point of contact for data subjects and the supervisory authority.

A compliant outsourcing partner will have a DPO that's certified by a body such as the International Board for IT Governance Qualifications (IBITGQ). The ICO provides a good outline of what a DPO should be.

3. Is their staff trained on technicalities of the GDPR? ☐ YES ☐ NO

Being compliant to GDPR is definitely an organisational responsibility, however, it's just as important that the offshore staff are well-versed with the main principles of information privacy in reference to GDPR.

Make sure that your outsourcing partner is taking all the steps required to impart GDPR-related knowledge to their staff at all levels. This means they have regular and in-depth training in addition to being audited by an independent standards body.

4. Do they have a registered office in the EU? ☐ YES ☐ NO

An outsourcing company is a data processor and if they are based in a country like India and process personal data of EU residents, they have to designate a representative in the EU. The representative must be registered with a Data Protection Authority (DPA).

5. Is the information security framework audited and certified by an external body? ☐ YES ☐ NO

Article 32 of the General Data Protection Regulation states that "the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk."

A GDPR compliant outsourcing firm will put in place security management systems such as ISO 9001 and 27001. Getting certified to the UK Government's Cyber Essentials scheme is also another method for establishing data security.

If you have any specific questions regarding the GDPR and outsourcing compliance you can ask our Expert DPO, Amit Simon.