DUE DILIGENCE CHECKLIST

# Due diligence checklist guidance

## How should I use my due diligence checklist?

Your company’s due diligence checklist is designed to provide you with a series of regulatory benchmarks from which to assess whether your suppliers are GDPR compliant. You should ensure you understand this information, complete the accompanying table, and store safely with your other GDPR documents, for safekeeping.

## Will I need to update my due diligence checklist?

Yes. It is your duty to ensure that other companies or suppliers you regularly work with are also GDPR complaint. You should request your suppliers answer the following questions, as outlined within this checklist. You should review this checklist at least every 12 months and amend as necessary, to ensure your company remains GDPR compliant.

# Introduction to your due diligence checklist

The following template offers a comprehensive checklist of the criteria you must assess to ensure your company’s suppliers are GDPR compliant. Any additional questions or need for clarification you may have for a particular supplier should be added to the bottom of this checklist as and when required.

|  |  |
| --- | --- |
| **Name of supplier** |  |
| Named supplier representative |  |
| Contact address of supplier |  |
| Review date |  |
| Scheduled date for next review |  |
| Name of company representative conducting check |  |

|  |
| --- |
| **Contract details information** |
| Are GDPR responsibilities defined within [COMPANY NAME’s] contract with the supplier? |  |
| Does the supplier take full liability in the event of a security breach? |  |
| Does the supplier take partial liability in the event of a security breach? |  |
| Has [COMPANY NAME] reviewed all contracts with the supplier? |  |
| Has the supplier defined GDPR responsibilities in their employment contracts? |  |
| **System security information** |
| Does the supplier take responsibility for data security? |  |
| Has the supplier documented its system coding and design? |  |
| Does the supplier carry out security testing on a regular basis? |  |
| Has the supplier taken all of the necessary steps to protect their systems? |  |
| Does the supplier encrypt data that is either ‘at rest’ or ‘in flight’?  (Note: this should include data exchanges such as email interaction or APIs.) |  |
| **Data subjects information** |
| Which individuals within the supplier’s business hierarchy have access to various data subjects? |  |
| What data can those authorised individuals access? |  |
| Why do those authorised individuals have access to that data? |  |
| Does the supplier use a ‘privacy by design’ approach in securing subject data? |  |
| What type of access and what rights to access does this supplier give to relevant data subjects? |  |
| **Data security information** |
| Is the supplier capable of fulfilling a subject access request? |  |
| What is the supplier’s process for fulfilling a subject access request?  (If applicable) |  |
| Does the supplier log changes to data? |  |
| Does the supplier report on logged changes to data? |  |
| Does the supplier implement right to be forgotten requests? |  |
| Does the supplier log right to be forgotten requests? |  |
| Does the supplier offer data portability in a usable format? |  |
| **Standards information** |
| Does the supplier in question observe ISO9001? |  |
| Does the supplier in question observe ISO27001? |  |
| Does the supplier in question have a Cyber Essentials certificate? |  |
| Does the supplier in question have C-base? |  |
| Is the supplier in question a member of the ‘Investors in People’ scheme? |  |
| **Financial information** |
| Has a satisfactory Companies House review of the supplier been successfully completed? |  |
| Has a satisfactory FCA/MOJ/ASA/ICO review of the supplier been successfully completed? |  |
| Has the supplier in question been administered a credit check? |  |
| Has the supplier in question passed a credit check? |  |
| Will the supplier indemnify [COMPANY NAME] in the event of a security breach? |  |
| **Insurance information** |
| Does the supplier in question have cyber insurance coverage in place? |  |
| Does the supplier’s insurance coverage extend to data protection? |  |
| Does the supplier’s insurance coverage extend to breach protection? |  |
| Does my supplier carry professional indemnity insurance? (yes/no) |  |
| **Privacy information** |
| Does the supplier in question restrict access to data to authorised personnel only? |  |
| Does the supplier encrypt data? |  |
| Has a security review been conducted of [COMPANY NAME]’s supplier systems? |  |
| Does the supplier ever use Open Source platforms? |  |
| Does the supplier in question audit the use of third-party plug-ins, themes or apps surrounding the use of Open Source platforms?  (If applicable) |  |
| **Data recovery information** |
| Does the supplier have a release management policy in place? |  |
| Does the supplier have a clearly outlined and clearly well-defined data recovery policy? |  |
| Does that data recovery policy include relevant protocols to ensure that no breaches occur if and when data must be restored? |  |
| Does the supplier have a data backup policy in place in the event of a system failure? |  |
| What does the supplier’s data backup policy procedure entail? |  |
| Does the supplier in question have a disaster recovery plan in place? |  |
| What does the supplier’s disaster recovery plan entail? |  |
| **Data breach information** |
| In the event of a data breach, does the supplier have a recording pathway? |  |
| What is the process by which [COMPANY NAME] will be informed of a data breach? |  |
| What is the process by which data subjects will be informed of a data breach? |  |
| What is the process by which relevant third parties will be informed of a data breach? |  |
| **Audit and reporting information** |
| Does the supplier in question offer any sort of audit of their services? |  |
| Is the supplier able to demonstrate their GDPR compliance? |  |
| How regularly does the supplier conduct reviews of the compliance? |  |
| Is the supplier able to provide an audit report demonstrating GDPR compliance? |  |
| **GDPR compliance information** |
| Based on the aforementioned checklist items, is the supplier in question GDPR compliant? |  |
| Has the supplier in question audited their own suppliers or vendors? |  |
| Does the supplier have a risk management process in place? |  |
| Does the supplier have an appointed Data Protection Officer? |  |

|  |
| --- |
| **Supplier due diligence checklist results – Fail/Pass/Additional information required** |

|  |
| --- |
| **Additional information required** |