

YOUR LOGO
GDPR COMPLIANCE MANUAL



INDEX

Foreword
Project Plan
GDPR Overview for Business Owners
KEY GDPR Highlights

Reference Documents

Reference documents contained in this section are drawn under licence from ICO, GCHQ and ACAS
[Copy of "Open Government Licence" to cover the inclusion of the ICO and GCHQ National Cyber Security extract reference documents in the manual](#)

1 Data Protection

Overview
ICO Guidance on Data Protection Officers
Data Protection Officer Responsibilities
Data Protection Law Review Procedure
ICO Guidance on Data Protection by Design and Default
GCHQ - National Cyber Security Centre Guide on Cyber Essentials for your Organisation

2 Lawful Bases for Processing Personal Data (overview and internal reviews)

Overview
ICO - Lawful Bases for Processing
[Company Names'](#) Procedures for any business processes involving the processing of personal data
Legitimate Interests Assessment Template
a) Asset mapping, GAP Analysis, Data Security Risk Assessment
b) Privacy Impact Assessment (PIA) Template and ICO Key Points on PIA's
c) Website GDPR statement and master "Consent" letter for Clients/Customers
d) Master Supplier Due Diligence letter and questionnaire, Template Third Party Supplier Agreement. Completed Due Diligence forms, copies of any supplier contracts/third party supplier processor agreements
e) [Company Names'](#) Revised internal forms accommodating the GDPR

3 Policies and Procedures

Overview
a) **General**
PRIVACY NOTICE
Data Protection Policy
Privacy Impact Assessment Procedure
Data Portability Procedure
Policy on Transferring of Personal Data to Third Party Countries/Organisations
Data Subject Access Request Procedure
Data Subject Access Request Record Form
Complaints Procedure
Professional Standards Authority – sample Retention and Disposal Policy
Secure Disposal Procedure

Company Name

Company Address

Company registration no

GDPR COMPLIANCE MANUAL

INDEX CONT...



- b) **Consent**
 - Consent Procedure
 - Ongoing Client Consent Letter and form
 - Ongoing Supplier Due Diligence and Consent letter and form
 - Parental Consent form
 - Removal of Consent Procedure
 - Data Subject Consent Withdrawal Form
 - Parental Consent Withdrawal Form
 - ICO Guidance on Children
 - c) **Staff**
 - Privacy Notice – Employees
 - Privacy Notice - Candidates
 - IT Policy (incorporating rules on acceptable internet and email use)
 - Access Control Policy
 - Access Control Rules and Rights for Users
- 4 **Data Breach of Privacy**
 - Overview
 - ICO Guidance around Dealing with a Personal Data Breach
 - Internal Procedure for Reporting Weaknesses, Events and Personal Data Breaches
 - Internal Data Breach Notification Form/Register
 - Personal Data Breach Notification Procedure
 - ICO Data Breach Notification Form
 - <https://ico.org.uk/media/for-organisations/documents/2258298/personal-data-breach-report-form-web-dpa-2018.doc>
- 5 **Staff - Ongoing**
 - Overview
 - GDPR Staff Record sheet
 - GDPR Overview
 - GDPR Key Highlights
 - PRIVACY NOTICE
 - Data Protection Policy
 - IT Policy (incorporating acceptable internet and email use)
 - Access Control Rules and Rights for Users
 - Data Retention and Disposal Policy
 - How to password protect excel and word documents
 - Procedure for Reporting Weaknesses, Events and Personal Data Breaches Internally
 - PRIVACY NOTICE – EMPLOYEES
 - PRIVACY NOTICE - CANDIDATES