

Actus GDPR Client Briefing 2018



Actus GDPR Briefing for Clients

With the forthcoming changes in the law there is a requirement for all organisations to comply with the new GDPR guidelines around data processing. We have developed this guide to make things as easy as possible for Actus clients to be able to demonstrate compliance as needed.

The following aspects of GDPR are covered in this guide:

1. Updated contractual data protection clauses by Actus on behalf of clients with regard to the processing and storage of data
2. Enabling clients to clearly communicate with staff why and how they are processing their data
3. Configurable options that Actus can provide to help clients to manage and retain data in line with their stated policies helping them to remain compliant
4. Actus as a business – in-house GDPR practices

1. Updated Contractual Data Protection Clauses

Actus is the data processor and you, the customer are the data controller. GDPR requires both parties to take more responsibility around the nature and transparency of data processing for staff. Actus has to ensure that any third-party providers used for hosting or development are contractually compliant and the customer must communicate to staff the scope and nature of the processing.

The following extract from our T&C's makes this more explicit and section 2 of this document provides you with the information that you need to communicate with your staff. You can download the full T&C's at: <https://actus.co.uk/our-software-policies/>

6. CUSTOMER DATA

- 6.1 The Customer shall own all rights, title and interest in and to all of the Customer Data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of the Customer Data.
- 6.2 Actus shall follow stringent back up and archiving procedures for Customer Data as set out in its Back-Up Policy accessible at www.actus.co.uk/ In the unlikely event of any loss or damage to Customer Data, the Customer's sole and exclusive remedy shall be for Actus to use its reasonable commercial endeavours to restore the lost or damaged Customer Data from the latest back-up of such Customer Data maintained by Actus in accordance with the Back-Up Policy. Actus shall not be responsible for any loss, destruction, alteration or disclosure of Customer Data caused by an unauthorised third party.
- 6.3 Actus shall, in providing the Actus Software and other Actus Services, comply with its Privacy & Security Policies both accessible at www.actus.co.uk. Furthermore Actus shall assist the Customer in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators.
- 6.4 If Actus processes any personal data on the Customer's behalf when performing its obligations, the parties record their intention that the Customer shall be the data controller and Actus shall be a data processor and in any such case:
 - (a) Personal data is stored in the UK and will not be transferred or stored outside the UK by Actus unless specifically requested by the Customer in writing and the following conditions are fulfilled:
 - (a) the Customer or Actus has provided appropriate safeguards in relation to the transfer;
 - (b) the data subject has enforceable rights and effective legal remedies;
 - (c) the Customer or Actus comply with their obligations under the Data Protection Laws by providing an adequate level of protection to any Personal Data that is transferred; and
 - (d) Actus complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data.
 - (b) the Customer shall ensure that it is entitled to transfer the relevant personal data to Actus so that Actus may lawfully use, process and transfer the personal data in accordance with the Agreement on the Customer's behalf;

- (c) the Customer shall ensure that Authorised Users and any relevant third parties have been informed of, and have given their consent to, such use, processing, and transfer as required by all applicable data protection legislation including GDPR; for one or more of the following purposes only: Performance management and appraisal; absence management; HR Administration; Feedback, Talent Management or Regulatory Compliance including SMCR.
 - (d) Actus shall process the personal data only in accordance with these Terms and Conditions and any lawful instructions reasonably given by the Customer in writing from time to time; and
 - (e) each party shall take appropriate technical and organisational measures to protect against unauthorised or unlawful processing of the personal data or its accidental loss, destruction or damage.
 - (f) at the written direction of the Customer, delete or return Personal Data and copies thereof to the Customer on termination of the agreement unless required by Data Protection Law to store the Personal Data.
- 6.5 Without prejudice to the foregoing, both parties agree that in the performance of these terms and conditions they shall, without limitation, each comply with the Data Protection Act 1998, the Data Protection Directive (95/46/EC) and all applicable laws and regulations including the GDPR relating to the processing of personal data and privacy.
- 6.6 Actus will provide regular upgrades and enhancements to the services within the licence fee and may migrate Customer data to the most up-to-date version of Actus Software during the licence term at no additional cost to the Customer in order to optimise functionality and security.
- 6.7 The Customer consents to the Provider appointing Memset Ltd as a third-party processor of Personal Data under this agreement. The Provider confirms that it has entered or (as the case may be) will enter with the third-party processor into a written agreement incorporating terms which are substantially similar to those set out in this clause 6. As between the Customer and the Provider, the Provider shall remain fully liable for all acts or omissions of any third-party processor appointed by it pursuant to this clause 6. The Customer consents to the Provider appointing additional third party processors in accordance with this clause provided that the Customer is informed in writing of their appointment.
- 6.8 Without prejudice to the foregoing, both parties agree that in the performance of these terms and conditions they shall, without limitation, each comply with the Data Protection Act 1998, the Data Protection Directive (95/46/EC) and all applicable laws and regulations including the GDPR relating to the processing of Personal Data and privacy. For the purposes of the GDPR Schedule A sets out the scope, nature and purpose of processing by Actus, the duration of the processing and the types of Personal Data and categories of Data Subject.
- 6.9 Actus will provide regular upgrades and enhancements to the services within the licence fee and may migrate Customer data to the most up-to-date version of Actus Software during the licence term at no additional cost to the Customer in order to optimise functionality and security. In addition, Actus will regularly assess and evaluate the effectiveness of the technical and organisational measures adopted by it.

2. The scope and nature of data processing using Actus

The following document forms Appendix 1 of our T&C's and can be used to explain this to staff or relevant authorities. The term 'supplier' relates to Actus:

PROCESSING, PERSONAL DATA AND DATA SUBJECTS

1. PROCESSING BY THE PROVIDER

1.1 SCOPE

Personal data collected and processed via the software application of the Supplier in relation to some or all of the following HR or compliance related activities including but not limited to employee performance management and appraisal; talent management; absence management; professional development and feedback; storage of personal data for HR reporting and remuneration; Monitoring of regulatory compliance and assurance.

1.2 NATURE

The Supplier's software is being used to process data to allow the Customer to operate an online HR database and Employee Performance Management system for its staff.

1.3 PURPOSE OF PROCESSING

The purpose may include some or all of the following depending on the modules that the Customer has selected: Performance Management and Appraisal; Training & Development; Professional Revalidation; Feedback & Development; SMCR assurance and accreditation Other related HR recording and reporting.

1.4 DURATION OF THE PROCESSING

For the duration of the agreement.

2. TYPES OF PERSONALLY IDENTIFIABLE DATA

The following data may be held within the standard Actus system (this list may be subject to update)

- Employee ID
- First Name
- Last Name
- Job Title or Role
- Email address
- Gender
- Known as
- Hire Date
- Bespoke HRD fields as agreed with the client

Other Personal Data includes but may not be limited to:

- Objectives & Measures
- Feedback
- Appraisal data or ratings
- Personal development plan/career aspirations
- Department
- Location
- Other HRD fields if relevant

3. CATEGORIES OF DATA SUBJECT

Users of the Actus System

2. Actus Configuration Options to help you with GDPR compliance

We have developed 4 additional options to help you with GDPR compliance, please get in touch with your engagement manager if you would like a quotation to enable any of these:

(a) Data purging

GDPR requires organisations to decide how long they will store data for. This is down to the individual company and is reasonably flexible as long as the organisation has a clear policy on this. Actus can work with you to set up data purging for different data retained within the system to help you automate this in line with your policies.

(b) Obtaining consent on log-in*

If you want to be certain that all of your staff have given their consent for you to process their details using Actus in line with the specified nature and scope above we can set up a single or multiple use consent form pop up. This gathers permission when users log in and stores that as a record.

**Please note this may not be available to SSO users*

(c) HR Database bespoke encryption

The Actus database functionality can be configured specifically for you to document individual understanding and responsibilities around GDPR or any other kinds of compliance and report on this. Sensitive personal data fields are encrypted as standard and additional fields can be encrypted on demand.

(d) Training logs

The development module within Actus allows you to document GDPR awareness training including dates it took place or when it expires and report on this or set reminders, helping you to maintain compliance.

Actus the business is ISO27001 Certified in its own right, therefore many of the established security process already meet the needs of GDPR. You can view our standard security policy here:

<https://actus.co.uk/our-software-policies/>

3. Actus as a business – our own GDPR practices

Clearly as a business in our own right we adhere to our responsibilities under GDPR for our own staff, clients and prospects in line with ICO guidance.

Our contract, combined with T&C's and sign off provide us with formal consent to remain in contact with our clients for the purpose of supporting them with the use of Actus, informing them of new developments and providing training, consultancy and education.

We set up GDPR compliant contracts with any third-party suppliers that we utilise for the development and support of Actus.

From a marketing point of view, we operate an 'opt in' only marketing policy and focus on providing value-add content. Our CRM System and Marketing Automation System allow us to monitor and respond to any 'opt in' or 'unsubscribe' requests.

As a business, we continue to monitor the guidance issued from the ICO and will update this statement and our processes as appropriate.