

Cloud9 Software – Summary of GDPR Compliance (As Data Processor)

Last Updated March 2018

With the introduction of new European Union (EU) legislation, due in May 2018, regarding the collection, storage and processing of personal data, Cloud9 Software (C9S) has been working to ensure that the Intelligentschedule.com service is compliant in advance of its introduction. The General Data Protection Regulation (GDPR) is due for introduction across the EU in May 2018 and places additional obligations on Data Processors of personal data.

At Cloud9 Software we take these obligations very seriously. We have produced this short summary paper to outline how we will fulfil our GDPR (as Data Processor) Obligations. Below are the key GDPR obligations for data processors and how C9S fulfils each.

Establish a representative in the EU, if the organisation is not located within the EU (in accordance with Article 27)

Because Cloud9 Software Limited is based in Liverpool, United Kingdom, we are not required to nominate a Representative. Our registered address is: 95 South Road [2nd Floor], Waterloo, Liverpool, United Kingdom, L22 0LR.

Each of our customers that reside outside the EU must nominate a representative that resides within the EU. This can be done by any administrator (including the key user) of the Intelligentschedule account navigating to the Configuration menu. There is a section named "Data Protection". In this section, you are able to nominate the name and contact details of your EU Representative.

Only Act on the written instructions of the controller (Article 29)

We commit to only complete any data related actions with the written instructions from the nominated key user for each customer account. This instruction will be accepted either electronically (email, helpdesk ticket response) or in written form. If the key user is no longer available at the customer organisation, we provide an offline process for the nomination of a new key user. Please contact support for more information about this process.

Implement and Comply with an Adequate Data Processing Agreement (DPA)

C9S has re-worked the terms of service and privacy policy associated with the service and introduced a GDPR compliant data processing agreement (DPA) associated to the terms of service and privacy policy. We explicitly name our sub-data processors. All versions of our terms of service are GDPR compliant from September 2017 onwards. The latest versions can be found here:

Our terms of service: <https://www.intelligentschedule.com/terms-of-service.html>

Our Privacy Policy: <https://www.intelligentschedule.com/privacy-policy.html>

Our data processing agreement: <https://www.intelligentschedule.com/data-processing-agreement.html>

Our list of data processors: <https://www.intelligentschedule.com/sub-processors.html>

Nominate a data protection officer in accordance with Article 37

Cloud9 Software Limited has nominated Paul Darlow (Director) as our Data Protection Officer. He can be contacted by email (paul.darlow@cloud9software.co.uk), by Phone (+44 (0) 151 928 8811) or by writing to 95 South Road (2nd floor), Waterloo, Liverpool, United Kingdom, L22 0LR.

Each of our customers must nominate a data protection officer. The data protection officer will be notified if there is an incident. This can be done by any administrator (including the key user) of the Intelligentschedule account navigating to the Configuration menu. There is a section named "Data Protection". In this section you are able to nominate the name and contact details of your data protection officer.

Restrict the appointment of sub-data processors (Article 28.2)

We maintain a list of Sub-data processors that support the intelligentschedule.com service. As part of the terms of service, the data processing agreement details the current list of sub-processes. The current list of data sub-processors can be found here:

<https://www.intelligentschedule.com/sub-processors.html>

If C9S add a new data sub-processor we will notify the key user and the nominated data protection officer (which may be the same person) of each account by email of the details (country of operation, purpose and name of service/organisation) of the new data sub-processor. Each customer has the right to not accept any new data processor and they will be able to terminate their use of the service.

Keep a Record of Processing activities in accordance with Article 30.2

Cloud9 Software is obligated to keep records relating to the processing of data as part of the intelligentschedule.com service. Specifically, we maintain:

- the name and contact details of the key user and the data protection officer for each customer; and
- A list of third countries (i.e. our sub-processors' locations) that personal data may be transferred to

Co-operate with the Supervisory Authorities (such as the ICO) in accordance with Article 31

We are committed to fulfilling our data processing obligations under the GDPR rules. As such we commit to cooperate and comply with all instructions issued by a GDPR supervisory authority.

Implement Adequate Data Security in accordance with Article 32

In addition to security processes (both physical and electronic) offered by our hosting partner (Amazon Web Services), Cloud9 Software has active Data Security Policies and Procedures. This includes our Business Continuity Plan. On an annual basis, all key staff are required to undertake Data Security training. As part of this annual session we also take the Opportunity to review the policies and procedures and update them if required. A summary of the current security policies and procedures can be found here:

<https://www.intelligentschedule.com/data-security.html>

Notify personal data Breaches to the Data Controller

For each of our customers we maintain the name of the Key user. In addition, we ask our customers to nominate a data protection officer. This may be the same person. In the event that we become aware of a data breach, we will inform both the nominated key user and data protection officer for each customer. We will communicate by email detailing the nature of the data breach and, if we are aware, detail the scope of the breach. We will communicate as soon as practically possible. It is the responsibility of our customers to update C9S if the key user or the data protection officer details we hold (including incorrect email addresses) change.