RACS Group & GDPR

Introduction

As the GDPR deadline approaches we understand that many of our clients are concerned about GDPR compliance in their organisation and with their suppliers.

For the past 9 months RACS have worked hard to audit our processes, contracts and notices. Key staff have attended external training courses and we have implemented a training plan for all staff. We are confident that we have taken all necessary steps to ensure compliance with the legislation before its inception on 25 May this year.

The main challenge for the recruitment industry is the right to process data on individual candidates/ workers and the legislation sets out the acceptable principles under which personal data can be held. We have reviewed the typical circumstances under which RACS receives, processes, transfers and holds an individual worker's data and established how we can do so compliantly under the new rules.

We will be communicating to all workers that we have updated our Privacy, Data Processing and Retention Policies (which they should read) prior to the 25 May.

Controller or Processor?

RACS's data processing activities exceed those of a processor (as defined by the legislation) and therefore we are a Data Controller and RACS will meet its obligations under this role.

RACS Compliance with each of the GDPR principles

Lawfulness, fairness & transparency

RACS has in place contracts of employment with its employees and policies which describe what categories of personal data are collected and processed and the lawful basis for doing this.

Personal data held on the RACS platform about individual Data Subjects is there for the purposes of fulfilling our:

- Contractual obligations under the contract of employment with the contractor,
- Legal obligations as employer in relation to HMRC, NMW/NLW compliance, pension obligations, gender pay gap reporting and the Criminal Finance Act
- Legitimate business interests under our supply agreements with agencies

Data minimisation

RACS captures most personal data in specific pre-determined fields which correspond to those defined in contract. Where documents are uploaded (e.g. identity documents) these are done so to facilitate specific performance of contractual obligation or to fulfil a legal obligation.

Accuracy

Some personal data can be corrected by workers within their secure access portal. Additional access, correction or deletion requests, can be actioned via specific email addresses set up for GDPR.

Data Retention Policy

In summary, where workers have been paid, RACS must hold their personal data for six full tax years following the end of the last tax year in which they were paid in order to comply with HMRC and pension record keeping requirements. We will communicate to workers that we will follow these data retention rules from 25 May onwards:

info@racsgroup.com 0345 604 0571 racsgroup.com

a) If we have processed a placement or payment(s) for the worker we will retain their personal data for a period of six tax years following the end of the last tax year in which they were paid, at the end of which period it will be deleted from our systems. We are required to retain their data and it cannot be deleted.

b) If we have not processed a placement or payment(s) for the worker, but they have provided us with personal data and accepted our data processing terms, we will retain their personal data for a period of 12 months, at the end of which period it will be deleted from our systems, unless they refresh their agreement to our data processing terms. They can request deletion of all of their data at an earlier stage.

c) If we have not processed a placement or payment for the worker, but they have provided us with personal data and not accepted our data processing terms, we will retain their personal data for a period of six months, at the end of which period it will be deleted from our systems, unless they subsequently indicate their agreement to our data processing terms. They can request deletion of all of their data at an earlier stage.

d) If we have not processed a placement or payments for the worker, but we received their personal data from a third party to whom they provided it (e.g. a recruitment agency) and they have not accepted our data processing terms, we will retain their personal data for a period of one month, at the end of which period it will be deleted from our systems, unless they subsequently indicate their agreement to our data processing terms. They can request deletion of their data.

e) Where a worker whose data is due for deletion subsequently updates their agreement to the RACS data processing terms this has the effect of renewing the compliant period to 12 months (as per 'b' above). Each month RACS systems will identify workers who data is due for deletion. They can request deletion of their data.

Accountability

RACS is fully capable of tracking data processing through our secure systems and provide compliance confirmation to regulatory bodies or as required contractually.

Integrity & confidentiality

RACS adopts various technical and organisational measures to prevent:

- Accidental or unlawful destruction, loss or alteration of personal data
- Unauthorised disclosure, transmission or processing of personal data
- Cyber penetration or hacking

RACS carry out regular vulnerability testing of our systems to ensure all data remains secure. We are in the process of applying for Cyber Essential Plus and will thereafter apply for ISO27001. RACS already apply the following principals to maintain the integrity and confidentiality of our data.

Asset Management:

- All assets are clearly identified and documented regularly (annually) in an asset register
- All assets designated owners/custodians listed in the asset register
- All employees must use company assets according to the acceptable use of assets procedures

Access Control

Access control is the selective restriction of access to a physical site or other resource. RACS operates controls across all electronic forms of information processing systems including operating systems,

applications, networks and mobile access to platform.

Procedures cover:

- User registration and de-registration
- Access privilege assessment
- Control of password use, password change and password removal
- Management review of access rights
- Network service access, control method for authentication of remote users
- Configuration of ports, segregation of networks

User Registration

RACS procedures:

- Staff users have a unique user ID based on a standard naming convention
- Formal authorisation process for provisioning of user IDs
- Audit trail available of all requests to add, modify or delete user accounts/IDs
- Access rights are immediately revoked for any employee leaving RACS
- Privileges are allocated to individuals on a 'need-to-have' basis
- Records of privilege accounts are maintained and updated on a regular basis

Operating system and application control policies include:

- All users in the organisation have a unique ID
- No systems or application details are displayed before log-in
- The number of unsuccessful log-in attempts is limited to 5 attempts
- During log-in process, all password entries are hidden by a symbol
- The use of system utility program is restricted
- The platform has a dedicated administrative menu to control access rights of users

Network security assurance

- Access to company's network is only provided to authorised users
- Controls are in place to manage remote users
- All equipment can be recognised uniquely
- Networks are segregated based on needs
- Network routing protocols are enabled
- Authentication mechanisms are used to control the access by remote users
- Allocation of network access rights is provided as per the business and security requirements

Compliance with data subject access rights

1. Right to be informed: RACS will notify the data subject when their information has been received

from self-registration or provision by third party, as soon as it is added to the platform.

2. Right to access: subject access rights may be met by the secure user portal (GDPR best practice). Requests can also be made via the dedicated email address set up for GDPR access requests.
3. Right to correct data: either directly on their secure user portal or via the dedicated email address for GDPR corrections.
4. Right to erasure of personal data: requests can be made using the dedicated email address for GDPR erasure. Rules are applied according to the data storage guidelines above.
5. Right to data portability: RACS provides personal data to the data subject in CSV file format.

Other compliance obligations

1. Transfer of data outside the EU: Where we have supplied data to agencies as Data Controller and the agencies wish to process or transfer this data outside of the EEA they will have to secure separate consent directly from each worker.
2. Data Protection Officer: RACS has appointed Jonathan Poole as DPO.
3. Sensitive data: As a default, RACS will not be handling sensitive personal data for the normal purpose of its service provision. RACS must be informed if sensitive personal data is required to be processed.

If you have questions relating to GDPR please email **GDPR@racsgroup.com**

info@racsgroup.com 0345 604 0571 racsgroup.com