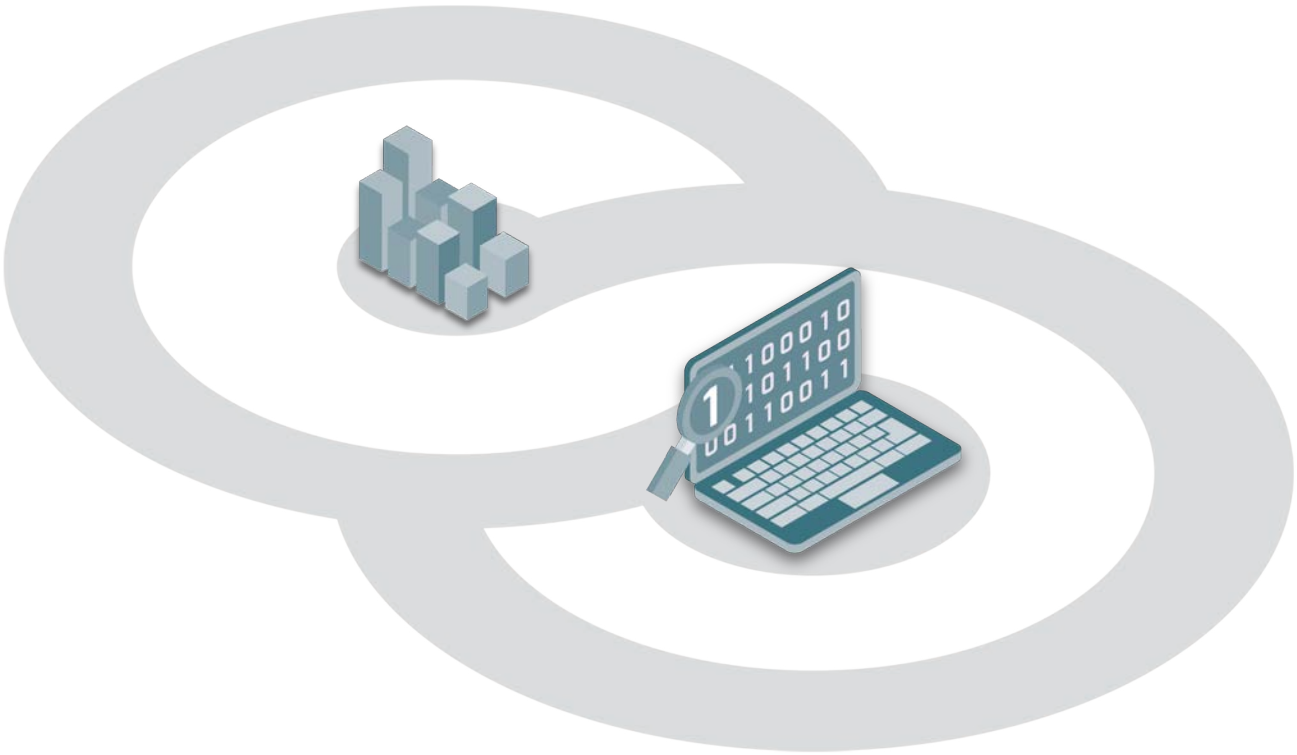
# UKCloud and the EU General Data Protection Regulation

## Addressing the requirements of GDPR and its post-Brexit UK equivalent




ukcloud | white paper

Making transformation happen.
T 01252 303 300
ukcloud.com

# Introduction

The European Union General Data Protection Regulation (GDPR), effective 25 May 2018, updates existing data protection laws for the digital age. It aims to:

- Harmonise data privacy laws across Europe
- Better protect EU citizens (data subjects) from privacy and data breaches
- Reshape the way organisations throughout the EU approach data privacy

To maintain information sharing, business relationships and data flows with the EU post Brexit, the UK is updating its own data protection laws to keep them closely aligned to GDPR. As a result, the rights of UK citizens, and the obligations on UK organisations to keep their personal data secure, will remain essentially unchanged once the UK leaves the EU.

UKCloud has been actively preparing for GDPR since 2016. In this paper we:

- Outline the roles and responsibilities of our customers as data controllers, and ours as their chosen data processor
- Give an overview of the rights of citizens as data subjects
- Describe how we will support our customers in achieving their own GDPR compliance

## In this white paper

# Data controllers and data processors: roles and responsibilities

In GDPR terms, our customers are the data controllers responsible for the personal data which is managed, processed or stored within their UKCloud environments.

UKCloud is their chosen data processor, undertaking data processing on their behalf, in accordance with their instructions as the data controllers.

We are committed to helping our customers meet their obligations as data controllers towards their data subjects.

## Ensuring GDPR compliance

Each data controller must ensure that appropriate organisational and technical safeguards are in place to enable compliant processing of personal data.

The data controller is responsible for:

- Determining the legal basis under which the processing of personal data is undertaken
- Obtaining any necessary prior consent, if applicable
- Selecting a data processor who can demonstrate compliance with GDPR data protection principles

## Contract requirements

A data controller must have a contract in place with its data processor that meets GDPR requirements. The contract must state the details of the data processing activities required, and set out the processor's obligations, including:

- The standards the processor must meet when processing personal data
- The permissions it needs from the controller relative to that processing

A Crown Commercial Service (CCS) guidance note[1] for government buyers explains how to bring commercial arrangements concerning data processing into line with GDPR.

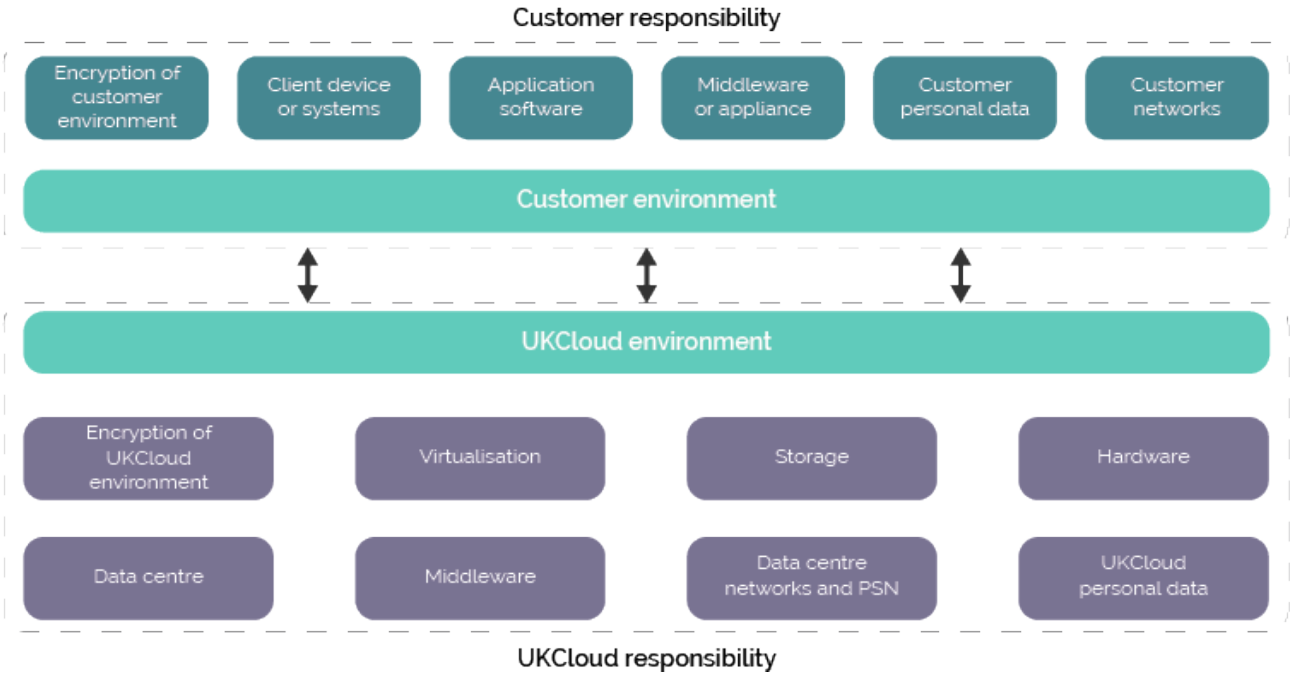
## Data processing instructions

As the data controllers responsible for the personal data which is managed, processed or stored within their UKCloud environments, our customers must provide us with unambiguous documented processing instructions explaining the responsibilities and expectations of UKCloud as their data processor.

As the data processor, we will act only on these documented instructions.

1 https://www.gov.uk/government/publications/procurement-policy-note-0317

**Figure 1. UKCloud and customer GDPR responsibilities**



# The rights of data subjects

GDPR strengthens and enhances the rights of data subjects and obliges data controllers to make a wide range of information available to them. That information includes published processes relating to data subjects' rights to:

- Access and validate their personal data, and understand why it's being processed
- Amend their personal data, if it's found to be incorrect or incomplete
- Receive their personal data and have it transmitted to another processor (data portability)
- Restrict or object to the processing of their personal data in certain circumstances
- Erase their personal data (right to be forgotten) in certain circumstances

To help our customers meet their obligations as data controllers towards their data subjects, we have already created and implemented processes that address each of these rights.

Data subjects who wish to exercise any of the rights outlined above will send their requests directly to the data controller, who is responsible for validating their identity and then providing a response.

We will co-operate with and support our customers — when asked to do so and when it's technically feasible — to help them meet their obligations as data controllers when responding to data subjects' requests.

# Data minimisation principle

Our services enable our customers to comply with the important GDPR principle of data minimisation.

Our customers are responsible for:

- Identifying and recording the applicable retention periods for the information types they process and store
- Ensuring they deploy effective data sanitisation or erasure technologies when removing personal data which is no longer required

**To help our customers meet their obligations as data controllers towards their data subjects, we have created and implemented processes that address data subjects' rights.**

# Data breach notifications

If a personal data breach occurs, the data controller must notify the supervisory authority (the Information Commissioner's Office in the UK) within 72 hours of becoming aware of the breach.

We will support our customers in meeting their notification obligations by notifying them as quickly as possible if we become aware of a breach of the personal data which is managed, processed or stored within their UKCloud environments.

Our data breach notification will:

- Describe the nature of the personal data breach as far as possible, bearing in mind we don't have access into our customers' UKCloud environments or visibility of the personal data which is managed, processed or stored there
- Describe the likely consequences of the personal data breach
- Describe the measures that we're taking, or that the customer must take, to address the breach including, where appropriate, measures to mitigate any adverse effects
- Communicate the name and contact details of our Data Protection Officer or other contact who can provide more information

The customer is responsible for documenting personal data breaches and reporting them to the supervisory authority and any affected data subjects.

# The cost of getting it wrong

Organisations in breach of GDPR can be fined up to 4% of their annual global turnover or €20m (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements, such as a significant data breach, or not having sufficient customer consent to process their personal data.

There's a tiered approach to fines so, for example, an organisation can be fined 2% (or up to €10m) for not having their records in order, not notifying the supervisory authority and data subject about a breach, or not conducting a data protection impact assessment.

**Organisations in breach of GDPR can be fined up to 4% of their annual global turnover or €20m (whichever is greater).**

**You can contact UKCloud's Data Protection Officer at dpo@ukcloud.com**

# UKCloud's security foundations

Our long-standing rigorous information security and governance controls, data protection practices, platform resilience, and staff security vetting and training provide firm foundations for our GDPR readiness.

## UK location

Our cloud services — including the physical hosting premises, support locations and support personnel — are all based in the UK. We never transfer personal data for which our customers are data controllers outside of the UK.

## Cloud platform resilience

Our services are designed and implemented to ensure:

- Multiple layers of resilience and redundancy across all cloud platforms
- No single points of failure

This approach includes geographically resilient data centres and support locations; and diverse, redundant power and connectivity feeds. We also maintain secure disaster recovery locations that can quickly be made operational if required.

UKCloud customers are responsible for selecting and configuring cloud services to meet their own resilience requirements.

## Security of processing

Our platforms are tailored to meet the needs of the UK public sector, and already reflect the core GDPR principle of 'data protection by design and by default' (Article 25).

As the data processor, we do not:

- Have access to any customer data held on our platforms
- Carry out data profiling or automated decision-making within cloud services

## Accreditations and certifications

Our portfolio of accreditations, certifications and security validations includes:

- NCSC Pan Government Accreditation (on behalf of specific customers)
- PSN certification for all UKCloud services
- Home Office PASF Certification
- ISO9001 for Quality Management
- ISO20000 for IT Service Management
- ISO27001 for Information Security Management
- ISO27017 for Security of Cloud Services
- ISO27018 for Personal Data in Cloud Environments

We make supporting evidence from our assurance activities available to our customers. You can ask our Data Protection Officer for more information.

## Data Protection Impact Assessments (DPIAs)

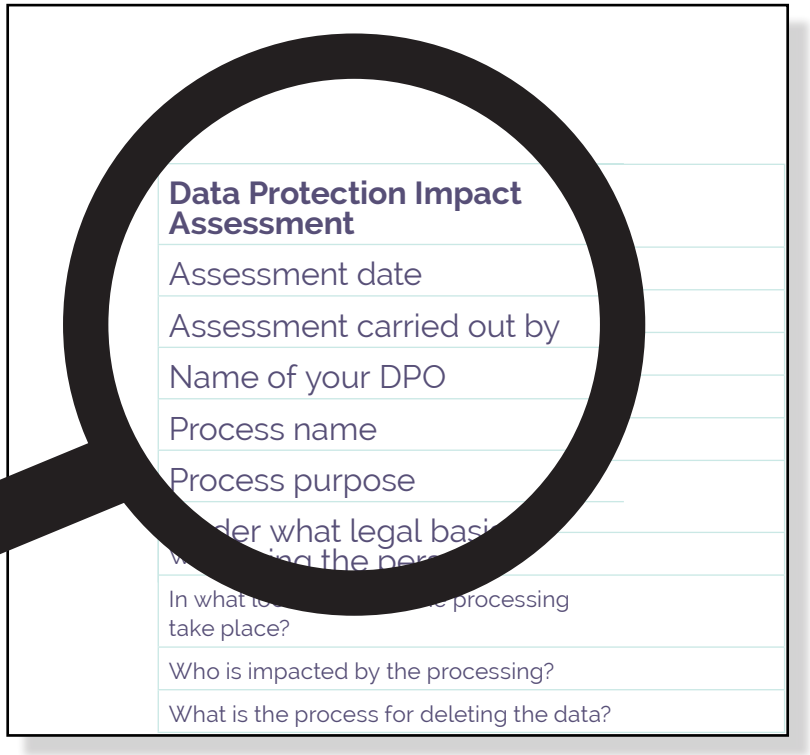
We have completed formal DPIAs for all processes within our organisation and for the cloud services used by our customers. These address the requirements of GDPR Article 35, which relate to data processing activities likely to result in a high risk to the rights and freedoms of natural persons.

Although GDPR doesn't require us to share DPIA reports, we promote transparency of our activities, and you can ask our Data Protection Officer for copies if required.

## Spotlight on DPIAs

GDPR Article 35 details the minimum requirement of a DPIA as follows:

- A systematic description of the planned processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes
- An assessment of the risks to the rights and freedoms of data subjects
- The measures intended to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR with regard to the rights of data subjects and other persons concerned.



## Personnel

### Confidentiality agreements

All UKCloud personnel sign employment terms and conditions that contain confidentiality requirements. They accept our platform Security Operating Procedures (SyOPs), which include additional confidentiality clauses and a declaration from the UK Official Secrets Act.

All our staff are subject to formal security clearance activities; members of staff with access to operational systems and data centre environments have SC and NPPV Level 3 clearances.

### Access to customer personal data

By default, none of our staff can access any customer's virtual environments. Any attempt to do so would be:

- Immediately detected and reported by our protective monitoring service
- Promptly identified and escalated as gross misconduct

If a customer requires technical assistance from a UKCloud analyst within their virtual environment, they must make a formal, approved and time-limited request, and monitor the intervention being provided throughout.

### Training and GDPR awareness

We train our staff on our approach to data protection with specific reference to GDPR requirements, and run a programme of data protection training and awareness workshops. Members of staff who have designated data protection tasks receive additional focused training.

### Data Protection Officer

Our Data Protection Officer (DPO) supports and advises the organisation, the executive team and the senior management team on GDPR compliance. Our DPO is also the point of contact for external parties (including regulators and data subjects) who wish to make enquiries or complaints about our data protection activities.

## Security of personal data processing

We use an Information Security Management System (ISMS) to manage information protection and formal assessments of the confidentiality, integrity and availability of both UKCloud and customer data. The ISMS is regularly validated by LRQA against ISO27001:2013, ISO27017:2015 and ISO27018:2014.

Our ISMS requires a formal approach to risk management and risk treatment that is validated during certification audits and allows for prompt identification of any unacceptable risks, which are then subject to remedial activities.

## Security controls

To provide effective protection against threats and vulnerabilities assessed within the ISMS, we have implemented technical, operational and personnel controls, drawn from ISO27001:2013, ISO27017:2015 and ISO27018:2014, which remove them, reduce the probability of them occurring, or reduce their impact if they were to occur.

Our customers are responsible for identifying and applying appropriate security controls within their virtual environments and applications, to ensure that any personal data being processed is protected in accordance with GDPR requirements.

## Security testing

Bi-annual IT Security Health Checks (ITSHC), requested by UKCloud and conducted by independent NCSC-approved CHECK providers, test our cloud services and the underlying infrastructure for technical and security vulnerabilities. The results are used as evidence to support our portfolio of security accreditations and certifications.

Our customers are responsible for arranging and conducting appropriate security tests within their virtual environments and applications to ensure that any personal data being processed is protected in accordance with GDPR requirements.

# Glossary of key terms

| Term | Description |
|---|---|
| **Data breach** | A data breach involves information being lost, stolen or compromised, or viewed without the owner's prior knowledge and authorisation. |
| **Data controller** | A person or body who determines the purposes and means of the processing of personal data, including the legal basis under which the processing is undertaken. |
| **Data processor** | An entity that processes personal data on behalf of a data controller, in accordance with the controller's formal written instructions. |
| **Data subject** | A natural person who can be directly or indirectly identified. |
| **DPIA** | Data Protection Impact Assessment. GDPR requires data controllers and data processors to conduct DPIAs before undertaking any processing activity that presents a specific privacy risk to data subjects. DPIA reports are often used to demonstrate privacy by design. |
| **DPO** | Data Protection Officer. GDPR requires organisations to appoint a DPO when:<br>• Data processing is carried out by a public authority, or<br>• The main data processing activities of the data controller or data processor<br>  • involve the regular and systematic monitoring of data subjects on a large scale, or<br>  • comprise large-scale processing of special categories of data or data about criminal convictions |
| **GDPR** | The European Union General Data Protection Regulation (2016/679). |
| **Personal data** | Any information relating to an identified or identifiable natural person (a data subject). |
| **Special category data** | As detailed in GDPR Article 9, specific categories of personal data which are more sensitive and need additional protection. |
| **Supervisory authority** | An independent authority responsible for monitoring the application of GDPR in an EU member state. The UK's supervisory authority is the Information Commissioner's Office (ICO). |

## Contacting our DPO

For more information about how we support our customers in demonstrating their GDPR compliance, contact our Data Protection Officer at dpo@ukcloud.com

# About UKCloud

UKCloud is dedicated to helping the UK Public Sector, delivering more choice and flexibility through safe and trusted cloud technology.

Since our inception, we have disrupted the market by producing innovative cloud solutions to meet the ever-evolving needs of the UK Public Sector. We're proud to have helped the sector save millions of pounds, delivering improved citizen services whilst supporting the growth of the UK digital economy.

We own and operate UK sovereign, industry leading multi-cloud platforms – offering security and assurance whilst being located within a Government-grade campus. Our platforms are open, making them easy to adopt, easy to use and easy to leave. They are underpinned by key technology platforms including VMware, Microsoft Azure, OpenStack, and Oracle.

## No one cloud fits all

Our multi-cloud platform offers choice and flexibility; we place the right workload, on the right cloud, in the right place. We do not lock you in to a single proprietary technology stack. We ensure that each solution runs on the platform most suited to delivering the best value and experience, and to meet the complex needs of the UK Public Sector.

## Built for the UK

We are home grown, home-owned and dedicated to serving the UK Public Sector. Our cloud platforms are all situated within the secure Government-grade Crown Hosting environment for non-cloud and multi-cloud services, all based in the UK – we call this Crown Campus.

## Making transformation happen

Using our expertise of having delivered more than 200 public sector digital transformation projects, our expert and trusted transition team helps customers understand the challenges they face and how they can navigate around them on the journey to the cloud and beyond.

## We help the UK Public Sector to make transformation happen through:

- Our belief in multi-cloud
- Focusing on the UK public sector
- Being open. You are never locked in
- Enabling collaboration within communities
- Accelerating your safe journey to the cloud

## More information

For more information about UKCloud and how we can help you, please send an email to info@ukcloud.com

## UKCloud. Making transformation happen.

**UKCloud Ltd**
A8, Cody Technology Park
Ively Road, Farnborough
Hampshire, GU14 0LX

**T** 01252 303 300
**E** info@ukcloud.com
ukcloud.com
@ukcloudltd



UKC-GEN-672-D • 02.2018