Our commitment to the General Data Protection Regulation

As an organisation that handles a considerable amount of data, ensuring we meet the requirements of local data protection laws as well as the GDPR is of paramount importance. We would like to take this opportunity to provide an update on the work we've undertaken to ensure that Logicalis is ready for the GDPR when it comes into force on the 25th May 2018.

Introduction

This document outlines how the Logicalis Guernsey Limited / Logicalis Jersey Limited and affiliated companies ("Logicalis") comply with the European Union's General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

Logicalis' data protection programme is designed to safeguard personal data according to the requirements of the GDPR. Its scope is to ensure:

i. It complies with data protection law and follows good privacy practices
ii. The protection of the privacy rights of data subjects whose data we have been entrusted with
iii. We are lawful, fair and transparent about how we process individuals' personal data
iv. We collect personal data for specified, explicit and legitimate purposes and do not further process them in a manner that is incompatible with those purposes
v. Personal data processed are relevant and limited to the minimum necessary in relation to the purposes
vi. Personal data are accurate, kept up to date where necessary and inaccurate data are erased or rectified without delay
vii. Personal data are kept in a form that identifies individuals for no longer than necessary
viii. Personal data are processed securely, protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures
ix. The risk and potential impact of data breaches is reduced to acceptable levels

At Logicalis, respecting and protecting privacy is of paramount importance, and is one of our key business principles.

How are we preparing for the GDPR?

Logicalis will be subject to the requirements of the General Data Protection Regulation (EU) 2016/679 both as a data controller as well as a data processor.

Logicalis is conducting a global GDPR readiness programme building on its commitment to comply with existing data protection legislation. This programme will ensure we meet our obligations to protect the rights and freedoms of individuals relating to personal data both in our capacity as data controller, as well as data processor on behalf of our customers.

Programme activities include an on-going review of risks, processing activities, information security management and technical controls, contractual relationships, staff training, education and awareness. This will also include implementing comprehensive data protection/privacy policies and procedures, such as records retention, subject access and incident management.

GDPR compliant data protection clauses within our contractual documents are currently under review - we will be contacting customers and suppliers in due course to ensure appropriate data processing agreements are put in place.

Additionally, we are currently underway with ISO27001 certification, having passed our stage 1 audit in December 2017 and expecting to gain certification in Q2 2018. We have a comprehensive ISO 27001 compliant Information Security Management Systems, with technical controls applied on the basis of risk management.

Client assessment questionnaires

We recognise and appreciate that our clients would like assurance around Logicalis' GDPR readiness. We would like to advise that Logicalis cannot complete client assessments at this time. Instead, we are providing this summary document to demonstrate Logicalis' GDPR current status and position on ensuring compliance as a Data Processor.

If you would still like us to provide a more detailed or customised response, we are more than happy to do so. However, we will need to charge a fee in order to cover the operational costs incurred in preparing this information.

Contract amendments & NDAs

We appreciate that clients may require formal agreements by means of amended contracts or non-disclosure agreements and we advise that we are unable to address individual requests in this respect.

To help our clients comply with the requirements of the Regulation and to cover our contractual requirements as a Data Processor we will shortly be issuing data processing agreements as addendums to our existing contracts. We will also be engaging in dialogue with clients/data controllers to inform us of their instructions around any data processing operations and to establish appropriate governance and controls on their personal data.

Data subjects' rights

The GDPR provides enhanced privacy rights for data subjects and fulfilment of those will be covered in our reviewed policies and procedures. We will provide details on who to contact for managing these types of requests (such as Subject Access Requests) and will engage with clients where necessary to support fulfilment of those requests within the mandatory timescales.

Lawful basis for processing

As Data Processor we intend to use the existence of our contract with you (the Data Controller) as the basis for any data processing we undertake. We will engage in dialogue with you to confirm this is the appropriate lawful basis for any data processing operations we undertake under your instruction.

Privacy notices

The content of Privacy Notices is your responsibility as Data Controller. We are happy to engage in dialogue with clients/Data Controllers if they have specific instructions or requirements around the provision of privacy notices for relevant data processing operations.

Privacy by design and by default

We are assessing the privacy and security considerations of our existing products and services and will be undertaking Data Privacy Impact Assessments on any new data processing operations, ensuring appropriate measures are in place to demonstrate that data protection has been integrated into data processing activities and new systems.

Incident management

We have a formal incident management process in place as part of our ISO27001 Information Security Management System. This is being reviewed to cover the requirements of the GDPR for incident monitoring, detection, response and reporting. Any suspected or actual personal data breaches affecting clients will be reported to them within the requisite timescales.

Data processing records

We have data processing logs in place which will include entries for personal data processed on behalf of clients. We will be engaging in dialogue with clients/data controllers to implement appropriate data processing agreements and part of this will involve making sure we have accurate information from data controllers on the nature of their personal data.

Security and Compliance

Logicalis has implemented and will maintain appropriate technical and organisational measures to ensure an adequate level of security that is appropriate to the risks it is aware of. We address security pro-actively to prevent accidental loss, destruction, alteration, unauthorised disclosure, access or unlawful destruction through five key activities:

1	Identify	Developing an understanding of the systems, assets, and data that need protection and the threats and risks to those systems
2	Protect	Implementing appropriate controls to ensure the security of our assets
3	Detect	Providing mechanisms to identify the occurrence of a security event
4	Respond	Taking appropriate actions when a security event is detected
5	Recover	Planning resilience and restoration capabilities for any services impaired due to a security incident

This aligns to multiple industry best practice frameworks and ensures Logicalis are able to keep ahead of the curve. The five key functions provide a solid foundation that Logicalis builds on to make a robust, layered security approach. Depending on the services you receive or subscribe to from Logicalis, additional technical and organisational measures may need to be implemented to ensure a level of security that is appropriate to the sensitivity and/or value of the data you are processing.

In all cases it is paramount we work together as data processor and data controller to ensure appropriate controls are implemented on your sensitive and valuable data.

What YOU should be doing now

- Review your risk management criteria
- Set up your personal data log/register
- Purge or delete unnecessary data
- Make sure you have an appropriate and practical retention schedule in place
- Review your sub-contractors and suppliers
- Summarise your technical and organisational security measures.
- Review your internal processes for ongoing compliance
- Provide training to staff on security awareness and data protection
- Ensure your contracts and NDAs are GDPR compliant
- Develop policies and procedures for fulfilling requests from data subjects
- Be aware of any automated decision-making and plan for objections
- Ensure you have appropriate insurance coverage