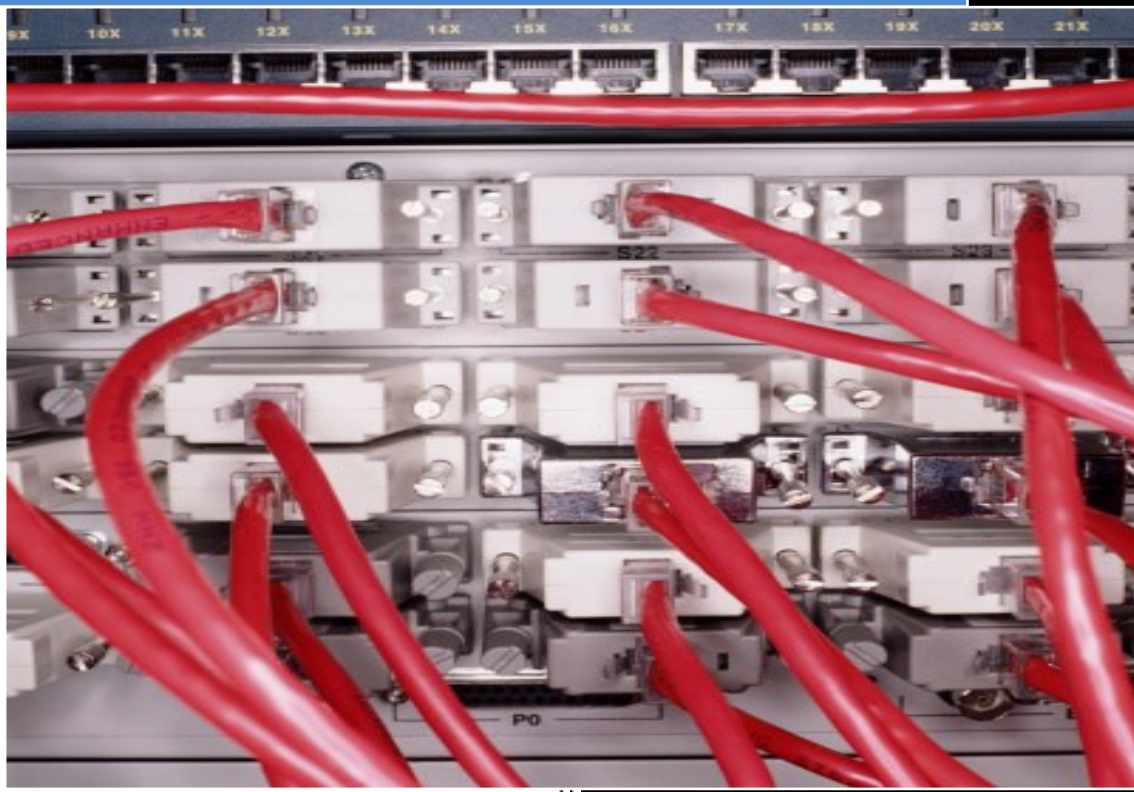
YourIT!
Your Logo Goes Here

GDPR Assessment

GDPR Compliance Questionnaire



Scan Date: 1/18/2018

Prepared for:
My Client Company
Prepared by:
YourIT Company

1/18/2018

Table of Contents

DATA PROTECTION OFFICER

GDPR requires that each organization designate a Data Protection Officer whose duties include informing and advising the organization on their obligations pursuant to the Regulation and act as the point of contact for the supervisory authority.

1.1 - DPO Name

Enter the name of the designated Data Protection Officer.

Joe Bloggs

1.2 - DPO Contact

Enter contact information to contact the designated Data Protection Officer.

123 Baker Street, London 5C7 86E, United Kingdom, email: jbloggs@neverflytoolanddie.co.uk

PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

GDPR lays out a particular set of principles to related to the processing of personal data. Use this questionnaire to indicate your understanding of these principles and that the personal data collected by your organization adheres to these principals.

2.1 - Lawfulness, Fairness, and Transparency

Personal data is processed lawfully, fairly and in a transparent manner in relation to the data subject

No

2.2 - Purpose Limitation

Personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')

No

2.3 - Data Minimization

Personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed

No

2.4 - Accuracy

Personal data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

No

2.5 - Storage Limitation

Personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject

No

2.6 - Integrity and Confidentiality

Personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

No

PERSONAL DATA USE

3.1 - Personal Data Use

Please state the reason for use of Personal Data from European Union persons. In each case of use, please indicate the purpose of the collection of data and if the data is the minimum necessary to achieve the processing goals.

Description of Personal Data	Processing Purpose	Is minimal?	Is consent provided?	How?
Company, Name, Address, Telephone Number, Email Address	Marketing	No	No	N/A

CHILD CONSENT

4.1 - Collection from minors

Does your organization collect data from children under the age of 16?

Yes

Follow-up to 4.1 if you answered Yes above
- Parental Consent

Do you acquire consent through the holder of parental responsibility?

No

SPECIAL CATEGORIES OF PERSONAL DATA

5.1 - Special Personal Data

Does your organization collect data that would reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation?

Yes

Follow-up to 5.1 if you answered Yes above
- Explicit Consent

Do you acquire explicit consent for such processing

No

PRIVACY POLICY REVIEW

To comply with requirements of GDPR related to obtaining consent from the data subject, the following items should be clearly identified within the information presented to the data subject at the time of consent. Please verify the following items are present in the policy.

6.1 - Policy Review

To comply with requirements of GDPR related to obtaining consent from the data subject, the following items should be clearly identified within the information presented to the data subject at the time of consent. Please verify the following items are present in the policy.

☐	Identity and Contact Details - the identity and the contact details of the controller and, where applicable, of the controller's representative.
☐	DPO Contact Details - the contact details of the data protection officer, where applicable.
☐	Purpose for Processing Personal Data - the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.
☐	Legitimate Interest - where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party.
☐	Recipients of Personal Data - the recipients or categories of recipients of the personal data, if any.
☐	Intent to Transfer (if applicable) - where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
☐	Retention Period - the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.
☐	Access and Erasure Rights - the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability.
☐	Right to Withdraw Consent - where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
☐	Right to Lodge Complaint - the right to lodge a complaint with a supervisory authority.
☐	Obligation and Consequences to Data Subject - whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

☐	Existence of Automated Decision-Making - the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
☐	Indirectly Obtained Personal Data Notice - notice that personal data obtained not directly from the obtained from the data subject also confirms to the above provisions.

REPRESENTATIVES OF CONTROLLERS OR PROCESSORS NOT ESTABLISHED IN THE UNION

7.1 - Non-EU Organization

Is your organization established outside of the European Union?

Yes

Follow-up to 7.1 if you answered Yes above
- Designated EU Representative

Enter the name and contact information of the designated representative within the European Union.

Rosemary and Thyme

PROCESSOR OR SUB-PROCESSOR

8.1 - Processors and Sub-Processors

For all processors or sub-processors involved in the process of personal data for natural persons from the European Union, you should review the contracts with those organizations to ensure they agree to comply with the principles and standards for data protection of GDPR.

Name and Contact Information of Processor	Contractually agrees to abide by GDPR
Google as the processor	No