TDL | CREATIVE

1 APRIL 2018

A PRACTICAL GUIDE TO THE GENERAL DATA PROTECTION REGULATIONS (GDPR)

TDL-Creative

TDL-Creative
St John's Studios
32A Larkfield Road
Richmond, Surrey
TW9 2PF

info@TDL-creative.com
www.TDL-creative.com

CONTENTS

INTRODUCTION

At TDL-Creative we take our data protection responsibilities seriously. We recognise that the introduction of GDPR from 25 May 2018 is a significant change in how we record our compliance with data protection law.

This guide is a practical explanation of the requirements of the GDPR as it applies to TDL-Creative and how we meet our obligations.

This document will be updated as necessary but in any event will form part of the annual review of company policies conducted by the directors.

Victoria Tomlinson, Managing Director, should be the primary source of advice and guidance to you on all of these matters.

Dated: 1st April 2018

SOME BASIC POINTS ABOUT 'WHAT' AND 'WHO'

- GDPR applies to personal data; in other words, any information relating to an identifiable person, no matter what format it is in. This includes obvious things like their name or address, but also something like their computer's IP address or other on-line identifiers.
- It does not apply to information relating to businesses as that is not personal data.
- It doesn't matter if the information is held in an electronic format on a computer system, or is held physically, such as on paper. The same rules apply to both.
- All such data is personal, but some categories of data are even more sensitive and require more secure handling.
- The 'Data Subject' is the person we hold information about.
- Someone who determines the purposes and means of processing personal data is known as a 'Controller'.
- Someone who is responsible for processing data on behalf of a Controller is known as a 'Processor'.
- GDPR applies to both Controllers and Processors.

WHAT DOES GDPR REQUIRE?

GDPR sets out the data protection principles that TDL-Creative must be responsible for and demonstrate compliance with.

The principles detailed in Article 5 of the GDPR require that personal data shall be:-

a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b. 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');

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d. 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 ('accuracy');

e. 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 ('storage limitation');

f. 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 ('integrity and confidentiality').

5(2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

WHAT DATA DOES TDL-CREATIVE DEAL WITH?

At TDL-Creative we have to deal with personal data. This falls into three categories:-

- Clients: To do our job, our clients provide us with relevant data about their customers so that we can deliver the services we provide. This relevant data can be personal data.
- Finance: We require personal data to deal with the billing and accounting tasks which follow from the above actions.
- Staff: Personal data is used to ensure that we meet our contractual obligations to staff and the related external bodies who we must share relevant data with, such as HMRC and other government departments, the pension provider, and such like. We also use personal data for monitoring purposes; for example, ethnicity is used in recruitment data.

WHAT JUSTIFICATION DOES TDL-CREATIVE HAVE FOR PROCESSING THAT DATA?

GDPR requires us to specify the valid lawful basis to process data. This differs depending on the type of data.

- Clients: We process custmer data to fulfil our contractual agreement with our clients to provide our services.
- Finance: The personal data we hold in respect of financial transactions is necessary to fulfil the contractual requirements of billing and payment.
- Staff: The personal data the company holds on each current individual member of staff is to comply with our legal obligations to HMRC and contractual obligations to staff; for example, in respect of pension provision. Data in respect of former members of staff is held for 7 years after they have left the employment of the firm. This time period is to ensure that the data is retained during the period when any claim for damages for breach of contract or personal injury has expired, including the time for issue and service of any claim form issued at the end of the primary limitation period.

SPECIAL CATEGORY DATA

This is personal data which is more sensitive and so needs more protection. It used to be referred to as 'sensitive personal data'. TDL-Creative do not require to process or obtain such data in order to carry out their business.

Where special category data on staff is held, for example in respect of health and union membership, this is processed pursuant to GDPR Article 9(2)(b) GDPR Article 9 (2) , or where that does not cover the situation then explicit consent is obtained in accordance with Article 9 (2)(a) GDPR Article 9 (2).

We demonstrate the lawful basis we have for processing data by publishing a Privacy Policy. This can be found on our website. We refer to this in the footer on our email and letterhead.

ACCOUNTABILITY AND GOVERNANCE

Everyone in TDL-Creative has responsibility for compliance with our data security obligations. Everyone must play their part but we have a hierarchy of responsibility.

- The Directors: have oversite of data protection and set/regularly review appropriate policies and define the purposes of processing data. They monitor compliance audit the effectiveness of the relevant activities and make changes in policy when required.

- Managers: each manager has specific responsibility to ensure that staff within their teams are aware of their responsibilities regarding data protection; that they follow company policies and report any issues arising or problems to the directors.
- Staff: must understand the data processing we do; follow company policies on how data is dealt with and security procedures as set out in our Information Security Policy (see staff handbook for further information), where it is needed and raise any problems or issues of concern with their manager.
- Suppliers: must act in accordance with the contractual terms we have in place with them. Our contracts are commercially sensitive so please speak to the design project manager should any specific matters need to be referred to.

SECURITY

A key principle of GDPR is that we process personal data securely by means of appropriate technical and organisational measures. The measures we take are designed to assure the confidentiality, integrity and availability of our systems and services and the personal data we process within them. We aim to prevent any accidental or deliberate compromise of the personal data we hold.

We have Information Security and Cyber Security Policies to explain to you the fundamentals of how to keep personal data secure and your role in achieving that. We also have a range of technical security measures in place as detailed in these policies.

INTERNATIONAL TRANSFERS

TDL-Creative does not transfer any personal data outside the European Union with the exception of data stored by the GDPR-compliant Dropbox Business file storage and sharing service that TDL-Creative uses.

PERSONAL DATA BREACHES

What is a Personal Data Breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This includes breaches that are the result of both accidental and deliberate causes. This could be, for example, sending personal data to an incorrect recipient.

Requirement to report to the ICO

We now have to report any breach which results in a risk to a person's rights or freedoms.

The managing director will assess all incidents to decide the likelihood and severity of any such risk and will report to the ICO accordingly. All such reports must be made within 72 hours of our becoming aware of it. If for any reason the managing director is unavailable during that timescale, the responsibility for filing a report will be delegated to another member of staff. Failure to report to the ICO can result in a very significant fine. It is essential that any breach incident is reported to the DPO immediately on discovery and without any delay at all.

What else do we do?

Reporting the breach to the ICO is not an end in itself. On becoming aware of any breach, immediate steps will be agreed so as to contain the breach and rectify the situation as far as is possible.

In some instances it may be necessary to notify the individual affected. This only arises if there is a 'high risk' to their rights and freedoms. Again it will be for the managing director to decide in each case whether there is a 'high risk'.

How do we learn from a breach incident?

An incident report will be prepared documenting the facts having investigated what happened; understood why it happened; the effects; the remedial action taken; and making recommendations for actions to avoid any repetition.

RETENTION OF DATA

We keep personal data for different time periods so as to comply with the principle that we keep personal data for no longer than is necessary for the purpose for which the personal data are processed.

- Staff: data is kept for seven (7) years after the end of their employment with the company.
- Job applicants: data is kept for 12 months after the completion of the recruitment process in which they were involved.
- Clients: data is kept for seven (7) years after the contract has expired to meet any legal obligations. After seven years any personal data not needed will be deleted.

A data audit is conducted annually so as to ensure that data is not being kept beyond the retention date.

APPENDIX 1 – PRIVACY POLICY

NOTICE: The Privacy Policy below will become effective May 25, 2018.

TDL-Creative cares about your privacy. For this reason, we collect and use personal data only as it might be needed for us to deliver to you our services. Your personal data includes information such as:

- Name
- Address
- Telephone number
- Date of birth
- Email address
- Usernames
- Password
- Other data collected that could directly or indirectly identify you.

Our Privacy Policy is intended to describe to you how and what data we collect, and how and why we use your personal data. It also describes options we provide for you to access, update or otherwise take control of your personal data that we process.

This document refers to personal data, which is defined as information concerning any living person (a natural person who hereafter will be called the Data Subject) that is not already in the public domain.

The General Data Protection Regulation (GDPR) seeks to protect and enhance the rights of data subjects. These rights cover the safeguarding of personal data, protection against the unlawful processing of personal data and the unrestricted movement of personal data within the EU. It should be noted that GDPR does not apply to information already in the public domain.

PERSONAL DATA

Tomlinson Designs Limited (t/a TDL-Creative) uses the information collected from you to provide quotations, make telephone contact and to email you marketing information which TDL-Creative believes may be of interest to you and your business. In you making initial contact you consent to TDL-Creative maintaining a marketing dialogue with you until you either opt out (which you can do at any stage) or we decide to desist in promoting our services. TDL-Creative also acts on behalf of its clients in the capacity of data processor. When working exclusively as a data processor, TDL-Creative will be acting on the instruction of its client and will take the reasonable necessary steps to ensure that the client is fully GDPR compliant.

Some personal data may be collected about you from the forms and surveys you complete, from records of our correspondence and phone calls and details of your visits to our website, including but not limited to personally identifying information like Internet Protocol (IP) addresses. TDL-Creative may from time to

time use such information to identify its visitors. TDL-Creative may also collect statistics about the behavior of visitors to its website.

TDL-Creative's website uses cookies, which is a string of information that a website stores on a visitor's computer, and that the visitor's browser provides to the website each time the visitor returns. The website analytics software in use therefore uses cookies to help TDL-Creative identify and track visitors and their website access preferences. Anonymous data collected by tracking cookies is stored for a period of 26 months before being removed.

TDL-Creative website visitors who do not wish to have cookies placed on their computers should set their browsers to refuse cookies before using TDL-Creative's website.

Any information TDL-Creative holds about you and your business encompasses all the details we hold about you and any sales transactions including any third-party information we have obtained about you from public sources and our own suppliers such as credit referencing agencies.

TDL-Creative will only collect the information needed so that it can provide you with marketing and consulting services, we will not sell or broker your data.

LEGAL BASIS FOR PROCESSING ANY PERSONAL DATA

To meet TDL-Creative's contractual obligations to clients and to also respond to marketing enquiries.

Legitimate interests pursued by TDL-Creative and/or its clients.

To promote the marketing and consulting services offered by TDL-Creative and/or to market the services and/or products offered by TDL-Creative's existing clients.

CONSENT

Through agreeing to this privacy notice you are consenting to TDL-Creative processing your personal data for the purposes outlined. You can withdraw consent at any time by emailing dpo@tdl-creative.com or writing to us, see last section for full contact details.

DISCLOSURE

TDL-Creative may on occasions pass your Personal Information to third parties exclusively to process work on its behalf. TDL-Creative requires these parties to agree to process this information based on our instructions and requirements consistent with this Privacy Notice and the GDPR.

TDL-Creative do not broker or pass on information gained from your engagement with the agency without your consent. However, TDL-Creative may disclose your Personal Information to meet legal obligations, regulations or valid governmental request. We may also enforce its Terms and Conditions, including investigating potential violations of its Terms and Conditions to detect, prevent or mitigate fraud or security or technical issues; or to protect against imminent harm to the rights, property or safety of TDL-Creative, its clients and/or the wider community.

RETENTION POLICY

TDL-Creative will process personal data during the duration of any contract and will continue to store only the personal data needed for [five years] after the contract has expired to meet any legal obligations. After five years any personal data not needed will be deleted.

DATA STORAGE

All the personal data we process is processed by our staff in the UK however for the purposes of IT hosting and maintenance this information is located on servers within the EEA. Unless required by law, we will not disclose your data to third parties.

YOUR RIGHTS AS A DATA SUBJECT

At any point whilst TDL-Creative is in possession of or processing your personal data, all data subjects have the following rights:

- Right of access – you have the right to request a copy of the information that we hold about you.
- Right of rectification – you have a right to correct data that we hold about you that is inaccurate or incomplete.
- Right to be forgotten – in certain circumstances you can ask for the data we hold about you to be erased from our records.
- Right to restriction of processing – where certain conditions apply you have a right to restrict the processing.
- Right of portability – you have the right to have the data we hold about you transferred to another organisation.
- Right to object – you have the right to object to certain types of processing such as direct marketing.
- Right to object to automated processing, including profiling – you also have the right not to be subject to the legal effects of automated processing or profiling.

In the event that TDL-Creative refuses your request under rights of access, we will provide you with a reason as to why, which you have the right to legally challenge.

TDL-Creative at your request can confirm what information it holds about you and how it is processed

You can request the following information:

- Identity and the contact details of the person or organisation (TDL-Creative) that has determined how and why to process your data.
- Contact details of the data protection officer, where applicable.
- The purpose of the processing as well as the legal basis for processing.
- If the processing is based on the legitimate interests of TDL-Creative or a third party such as one of its clients, information about those interests.
- The categories of personal data collected, stored and processed.
- Recipient(s) or categories of recipients that the data is/will be disclosed to.
- How long the data will be stored.
- Details of your rights to correct, erase, restrict or object to such processing.
- Information about your right to withdraw consent at any time.
- How to lodge a complaint with the supervisory authority (Data Protection Regulator).
- 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 you are obliged to provide the personal data and the possible consequences of failing to provide such data.
- The source of personal data if it wasn't collected directly from you.
- Any details and information of automated decision making, such as profiling, and any meaningful information about the logic involved, as well as the significance and expected consequences of such processing.

TO ACCESS WHAT PERSONAL DATA IS HELD, IDENTIFICATION WILL BE REQUIRED

TDL-Creative will accept the following forms of ID when information on your personal data is requested: a copy of your national ID card, driving license, passport, birth certificate and a utility bill not older than three months. A minimum of one piece of photographic ID listed above and a supporting document is required. If TDL-Creative is dissatisfied with the quality, further information may be sought before personal data can be released.

All requests should be made to london@tdl-creative.com or by phoning 020 3637 9961 or writing to us at the address further below.

CHANGES TO THIS PRIVACY POLICY

We reserve the right to modify this Privacy Policy at any time. If we decide to change our Privacy Policy, we will post those changes to this Privacy Policy and any other places we deem appropriate, so that you are aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. If we make material changes to this Privacy Policy, we will notify you by email, or by means of a notice on our home page, at least thirty (30) days prior to the implementation of the changes.

COMPLAINTS

In the event that you wish to make a compliant about how your personal data is being processed by TDL-Creative or its partners, you have the right to complain to TDL-Creative's [CEO]. If you do not get a response within 30 days, you can complain to the Data Protection Regulator.

The details for each of these contacts are:

Tomlinson Designs Limited (t/a TDL-Creative), for the attention of Oliver Tomlinson

St John's Studios

32A Larkfield Road

Richmond

Surrey

TW9 2PF

Telephone 020 3637 9961 or email london@tdl-creative.com

Data Protection Regulator:

Information Commissioner's Office

Telephone 0303 123 1113 or complete a form at: https://ico.org.uk/concerns/handling/

APPENDIX 2 – TEMPLATE FOR DATA BREACH REGISTER

Ref	Description of breach	date identified	Identified by	Remedial action to prevent recurrence	Reportable to ICO / other regularor?	Date reported to ICO / other regularor?	Date closed	Comments	Breach or potential breach

APPENDIX 3 – INFORMATION SECURITY POLICY

What this policy covers

This policy details your rights and obligations in relation to your personal data and the personal data of third parties that you may come into contact with during the course of your interaction or employment with TDL-Creative.

This policy applies to all employees (permanent and temporary) and any associates that use TDL-Creative's information and Communication Technology systems.

If you have access to the personal data of employees or of third parties, you must comply with this policy. Failure to comply with the Policy and procedures may result in disciplinary action up to and including dismissal without notice.

This policy must be read in conjunction with TDL-Creative's Cyber Security Policy, Guide to GDPR, and privacy policy.

INTRODUCTION

TDL-Creative are required to maintain certain personal data about living individuals for the purposes of satisfying operational and legal obligations. We recognize the correct and lawful treatment of personal data; it maintains confidence in the company and provides for successful operation.

Information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory and contractual obligations. Whichever format the personal data is stored or used, it will be subject to the appropriate legal safeguards as specified in the Data Protection Act 2018 and GDPR.

YOUR ENTITLEMENTS

Personal Data means data held either on a computer or in a paper-based filing system which relates to a living individual who can be identified from that data.

GDPR and The Data Protection Act 2018 prescribe the way in which TDL-Creative may collect, retain and handle personal data. TDL-Creative will comply with the requirements of these acts and all employees and contractors who handle personal data in the course of their work must also comply with it.

The purposes for which your personal data may be held by TDL-Creative

Personal data relating to employees may be collected by TDL-Creative for the purposes of:

- recruitment, promotion, training, redeployment and / or career development, such as references, CVs and appraisal documents
- administration and payment of wages, such as emergency contact details and bank/building society details
- calculation of certain benefits including pensions
- disciplinary or grievance issues
- performance management purposes and performance review
- recording of communication with employees and their representatives
- compliance with legislation
- provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers and
- staffing levels and career planning

Sensitive personal data

Sensitive personal data includes information relating to the following matters:

- your racial or ethnic origin
- your political opinions
- your religious or similar beliefs
- your trade union membership
- your physical or mental health or condition
- your sex life, or
- the commission or alleged commission of any offence by you

Processing of sensitive data

TDL-Creative will process sensitive data primarily where it is necessary to enable TDL-Creative to meet its legal obligations and in particular to ensure adherence to health and safety and vulnerable groups protection legislation or for equal opportunities monitoring purposes. In most cases, TDL-Creative will not process sensitive personal data without your consent.

PROCEDURE

Accuracy of personal data

TDL-Creative will review personal data regularly to ensure that it is accurate, relevant and up to date.

To ensure TDL-Creative's files are accurate and up to date, and so that TDL-Creative is able to contact you or, in the case of an emergency, another designated person, you must notify TDL-Creative as soon as possible of any

change in your personal details (e.g., change of name, address, telephone number, loss of driving licence where relevant, next of kin details, etc).

Security of personal data

TDL-Creative will ensure that personal data is not processed unlawfully, lost or damaged. If you have access to personal data during the course of your employment, you must also comply with this obligation. If you believe you have lost any personal data in the course of your work, you must report it to your manager immediately. Failure to do so may result in disciplinary action up to and including dismissal without notice.

When dealing with personal data, please make sure that all appropriate measures are taken to prevent loss, destruction, or corruption of data. The following are examples of everyday simple steps that can be taken in order to make sure we comply with our obligations to protect data and ensure confidentiality:

- Laptops or desktops containing access to personal data should not be left unattended when logged on and the screen cleared of any data when locked after use/unattended
- People who have access to the studio or offices where we're working should only be invited guests or authorized visitors. Personal data should not be left in any place which could be visible to visitors or guests.
- The meeting room must be cleared of any documents containing personal data at the end of any meeting. Similarly, desks should be cleared in the same way at the end of each day
- Security should be remembered/considered when discussing clients or staff with other colleagues. For example, extra care should be taken when discussing such matters when speaking on a mobile phone in public, for example
- Staff should be aware of and adhere to the Cyber Security Policy

Access to personal data ["subject access requests"]

The Data Protection Act 2018 and GDPR gives you the right to access the personal data held about you by TDL-Creative.

For further information, please see our Privacy Policy.

APPENDIX 4 – GDPR SECURITY CHECKLIST

As per the ICO's website and GDPR security checklist (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/), further details can be found below relating to each point in relation to TDL Creative's IT infrastructure and processes.

Analysis of risks presented by our processing

TDL-Creative encounters a number of risks when processing personal data as per any other UK business. These include virus attacks, spam, and location of data stored. For these reasons, the measures detailed in the next section have been implemented.

Measures implemented taking into account what's available in the marketplace and costs of implementation

The IT marketplace has many different products and offerings to safeguard a company's data and these are continually evolving – as are the threats posed.

TDL Creative has therefore assessed the available products and implemented the following reasonable, industry standard and what we believe are the best fit given the size of TDL-Creative and the data it processes:

- A secure and up-to-date firewall
- Up-to-date antivirus/spyware/software firewall monitoring software on all machines
- All personal data being securely stored within the EEA (including file storage and email services)
- Encryption of all laptop computers

Information security policy and confirmation of implementation

An information security policy has been introduced and staff have been informed about this. It can be found in the staff handbook.

Regular review of the above and assessing any improvements

The above are reviewed annually along with all security and IT-related policies and procedures.

Implementation of technical controls specified by frameworks such as Cyber Essentials

TDL-Creative are currently looking to apply for Cyber Essentials accreditation since we have been working hard over the past few months to make sure our IT infrastructure is compliant with this standard.

Other technical measures appropriate to the data that we process

These have been taken into account and a list of all technical measures that have been taken are detailed above.

Use of encryption and/or pseudonymisation

As above, all laptops are encrypted and the company data held by our storage provider on off-site servers is also encrypted at rest and in transit.

Understanding the requirements of confidentiality, integrity, and availability of the personal data processed

The requirements outlined above are fully understood hence the IT infrastructure setup and security software/backup routine that is in place.

Making sure that access to personal data can be restored in the event of any incidents with established and appropriate backup processes

Backups of data are taken regularly and stored securely. We are also able to restore data through our secure cloud storage provider for a period of 120 days following deletion.

Conducting regular testing and reviews of the measures to ensure they're effective and acting on any shortfalls established

In terms of data storage, our cloud storage provider provides a service which has been fully tested and is being constantly developed by them.

We are also constantly reviewing the marketplace in order to make sure we have the best technology available in relation to our size and budget.

Implementing measures that adhere to an approved code of conduct or certification mechanism

As above, we are looking into Cyber Essentials accreditation.

Ensuring that any data processor we are using also implements appropriate technical and organisational measures

We are striving to make sure that all data processors we use have the appropriate technical and organisation measures in place in order to meet our high standards.