ONE WORKS POLICY:
DATA PROTECTION POLICY

Introduction

One Works (including One Works Asia and One Works DMCC) acknowledge that everyone has rights with regard to the way in which their personal data is handled. One Works collects, stores and processes personal data about our employees and the employees, clients, suppliers and other third parties, and recognises that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

About this Policy

This policy applies to all individuals working within, and for, the One Works at all levels and grades, including directors, senior managers, staff, consultants, contractors, seconded staff, agency staff, agents or any other person associated with us or any of our subsidiaries or their employees, wherever located.

This policy, and the other documents referred to in it, sets out what we expect from you in order for One Works to comply with applicable law and you must read, understand and comply with this policy when processing Personal Data on our behalf. Compliance with this policy is mandatory and any breach may result in disciplinary action.

This policy, and any other documents referred to in it, also sets out the basis on which One Works will process any personal data it collects from data subjects, or that is provided to One Works by data subjects or other sources. It also sets out rules on data protection and the legal conditions that must be satisfied when One Works obtains, handles, processes, transfers and stores personal data.

The types of personal data that One Works may be required to handle include information about current, past and prospective employees of One Works, suppliers, contractors and clients (and their respective employees) and others that One Works communicates with. The personal data, which may be held on paper, electronically or in any other media, is subject to certain legal safeguards specified in data protection legislation in Europe and other jurisdictions, including the General Data Protection Regulation (GDPR) and other regulations.

Our Principles

Anyone processing personal data must comply with the data protection principles set out in the GDPR. These provide that personal data must be:

- Processed fairly and lawfully and in a transparent manner
- Obtained only for one or more specified, explicit and legitimate purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
- Adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which they are processed
- Accurate and, where necessary, kept up to date
- Not be kept in a form which permits identification of data subjects for longer than is necessary for the purpose or purposes for which it is processed

- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- Not transferred to or accessed by a country or territory outside the European Economic Area without appropriate safeguards being in place.

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above. The GDPR also gives data subjects a number of rights in relation to the data we hold about them (including rights to access their data) which we must respect.

You must email milan@one-works.com immediately if you suspect there has been a Personal Data breach or receive a Subject Access Request (SAR).

You should also refer to the One Works Compliance Manager if you have any concerns that the policy has not been followed or if you have any questions about the operation of this policy, such as:

a) you are unsure about the retention period for the Personal Data being processed
b) you are unsure about what security or other measures One Works has in place to protect Personal Data
c) you are unsure on what basis to transfer Personal Data outside the EEA
d) you have been asked by a client to provide Personal Data other than a CV or photograph as part of a bid or submission.

Fair and Lawful Processing

The GDPR is not intended to prevent the processing of personal data, but to ensure that it is done lawfully, fairly and in a transparent manner and without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the GDPR. These include, among other things, (i) the data subject's express and freely given consent to the processing, (ii) the processing is necessary for the performance of a contract with the data subject, (iii) the processing is necessary for the compliance with a legal obligation to which the data controller is subject (e.g. health & safety or employment laws), or (iv) for the legitimate interest of the data controller or the party to whom the data is disclosed, provided that this interest is not overridden by the interests of the data subject. When sensitive personal data (also known as ‘special category’ data) is being processed, additional conditions must be met (and data relating to criminal convictions must not be processed except in very limited circumstances). When processing personal data as data controllers in the course of One Works' business, One Works will ensure that those requirements are met.

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked
- Contact the One Works Compliance Manager for assistance in difficult situations. No-one should be bullied into disclosing personal information.

Consent

Consent is one of the lawful bases that we can use to process personal data. However, there are a number of conditions that have to be satisfied for consent to be effective and these are generally difficult to satisfy in relation to employees. Accordingly, it is our policy to avoid relying on consent as a basis for processing of data where another lawful basis (e.g. legitimate interests or compliance with a legal obligation) may be available.

From time to time, we may ask for your consent to process certain information about you which you can refuse, for example the use of your photograph in publicity material. If you agree, you can subsequently withdraw your consent to us doing so at any time by sending a request to the contact details at the end of this notice.

Where consent is intent to be relied on as the basis for processing data you must obtain guidance from the One Works Compliance Manager in advance by emailing milan@one-works.com.

Processing for Limited Purposes

One Works will only process personal data for the specific, explicit and legitimate purposes notified to the data subject when the data was first collected or for other purposes permitted by the GDPR. One Works will notify those purposes to the data subject when the data is first collected or at any point where personal data is processed for a purpose other than that for which the personal data was originally collected.

One Works will hold and process personal data about its employees in manual and automated filing systems as set out in the Employee Privacy Notice.

Where any services or benefits provided to One Works or the One Works Group by third parties, for example for: pension administration; health insurance/benefits, One Works may disclose employees' personal information to those third parties but will take reasonable steps to ensure that such data is held securely.

One Works may also process sensitive personal data (such as health data, data relating to ethnic origin, religious beliefs or data relating to the commission of an offence) about its employees where it is necessary, for example for: health administration; health insurance/benefits; and equal opportunities monitoring and as necessary for One Works to exercise its rights or perform its obligations under applicable employment law.

Notifying Data Subjects

Where One Works collects personal data directly from data subjects, we will inform them about:

- The purpose or purposes for which One Works intends to process that personal data,
- The types of third parties, if any, with which One Works will share or to which One Works will disclose that personal data to
- The means, if any, with which data subjects can limit One Works' use and disclosure of their personal data.

Adequate, Relevant and Non-Excessive Processing

One Works will only collect personal data to the extent that it is required for the specific purpose notified to the data subject or as otherwise permitted by the GDPR.

Accurate Data

One Works will endeavour to ensure that personal data it holds is accurate and kept up to date. One Works will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Employees are responsible for ensuring that they keep the following information up to date using YourData as relevant; name, address, personal email address, emergency contact details and bank account information. One Works will take reasonable steps to destroy or amend inaccurate or out-of-date data.

Timely Processing

One Works will not keep personal data longer than is necessary for the purpose or purposes for which they were collected or as otherwise permitted by the GDPR. One Works will take all reasonable steps to destroy, or erase from its systems, all data which is no longer required.

For more information on our data retention periods please contact us on the details at the end of this notice.

Data Subject's Rights

Data subjects may make a formal request for information, Subject Access Request (SAR), One Works holds about them. Any such request can be made in writing or verbally. Any such request must follow One Works' SAR procedure and be sent immediately to the One Works Compliance Manager.

One Works will process all personal data in line with data subjects' rights, in particular their:

1. The right of access – this enables individuals to receive further information about the personal data we hold about them as well as to obtain a copy of that data
2. The right to rectification – this enables individuals to have any incomplete or inaccurate personal data that we hold about them corrected
3. The right to erasure (also known as the 'right to be forgotten') – in limited circumstances an individual can ask us to delete personal data we hold about them, for example where it is no longer required for the purposes for which it was collected/processed
4. The right to restrict processing – in limited circumstances an individual can ask us to suspend the processing of their personal data
5. The right to data portability – in limited circumstances an individual can ask us to transfer their personal data to another organisation
6. The right to object – the enables an individual to object to us processing their personal information in limited circumstances.

Data Security

One Works will take reasonable security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

One Works will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if they have confirmed they comply with the requirements of applicable data protection legislation.

One Works will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on One Works' central computer system with appropriate filing security and not on individual PC hard drives.

Security procedures include:

- Entry controls. Any stranger seen in entry-controlled areas should be reported to the appropriate Office Manager
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential)
- Methods of disposal. Paper documents should be shredded or disposed of in the studio confidential waste bins provided. Digital storage devices should be cleared down in a secure manner or physically destroyed when they are no longer required
- Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock their PC when it is left unattended.

As set out in the One Works Use and Misuse of IT, Communications and Systems Policy, One Works will monitor user activity on the Internet at network level for the purposes of security and integrity of the One Works' network. This extends to PCs, laptops and personal devices connected to the One Works network both wirelessly and on occasion through wired connections. Monitoring also continues of One Works devices when used remotely, with user activity automatically reviewed when devices are next connected to the network. This includes user identification (SSID and IP address), domain names of websites visited, duration of visits, and all files downloaded from the Internet. Staff should be aware that this monitoring may reveal sensitive data about them, for example visits to websites which detail the activities of a particular political party or religious group might indicate the political opinion or religious belief of that individual. Staff should maintain their own personal privacy by not using One Works' systems to access this type of information. Staff should also acknowledge that all internet activity logs are regularly backed up with records maintained as necessary for the stability and robustness of One Works' overall IT systems.

It is important to note that One Works policies, including this one, apply to all One Works supplied devices (laptop, smartphone and tablet) whether used inside or away from the office and any personal devices connected to any One Works network.

Transferring Personal Data to a Country outside the EEA

One Works may transfer personal data to (or allow access to it from) countries outside the European Economic Area (EEA) including but not limited to One Works Group's personnel based in China, India, Canada and the Middle East. We have in place agreements between our group companies to ensure your personal data is treated by all of our Group companies in a way that is consistent with EU and UK data protection laws.

Countries outside of the EEA may not have data protection laws as comprehensive as those existing in the EEA. One Works and the One Works Group will take reasonable steps to ensure that an adequate level of protection is in place in relation to the transfer and processing of such personal data outside of the EEA.

ONEWORKS:

Disclosure and Sharing of Personal Information

One Works may share personal data we hold with any member of our group. One Works may also disclose personal data it holds to third parties:

- With our brokers, agents, insurers and/ or professional advisors for the placing of benefits and insurances
- With other companies within the current, and future, Group for project collaboration and intercompany transfers
- With other third-party contractors who provide services to us in relation to insurance benefits and suppliers of our IT systems when required to enable them to provide services to us. Further information is available from local HR
- With clients and potential clients where it is required to enable us to provide a service to them and to respond to tenders
- In the event that One Works sells or buys any business or assets, in which case it may disclose personal data it holds to the prospective seller or buyer of such business or assets
- To third parties where required to protect One Works' rights, property, or the safety of One Works employees, clients or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction
- To police, government and other regulatory authorities where we are required to do so or we are requested to do so and we consider it is appropriate to do so in the circumstances.

Review and Monitoring of this Policy

This policy, which is non-contractual, will be monitored periodically by the One Works Compliance Manager to ensure it is up to date and achieving its objectives and may be amended from time to time.

Responsibility for the Policy

For the purposes of this policy, the Compliance Manager will have primary responsibility for the regular review and update where appropriate. The responsibility for the appropriate and effective application of the policy across each studio is with the Partner and/or Office Manager.

This is One Works' Data Protection Policy and as Managing Partner I commit myself and the company to it.

Leonardo Cavalli
Managing Partner

Updated: 1 September 2018