Privacy Policy
INTERNAL DATA PROTECTION POLICY

SINE QUA NON PICTURES LIMITED
(THE "Company", "WE", "US" AND "OUR")

LAST UPDATED: 20TH NOVEMBER 2019

DEFINITIONS AND INTERPRETATION

In this Policy, the following terms have the following meanings:

Automated Decision-Making: when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company Personnel: all of the Company's employees, workers, contractors, agency workers, consultants, directors, members and others whom it engages in an employment context from time to time.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: personal data relating to criminal convictions and offences.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Protection Legislation: the GDPR, the Data Protection Act 2018 and any other applicable data protection legislation from time to time in force.

Data Protection Contact: this term means a data protection manager or other voluntary appointment of a Data Protection Contact or refers to the Company's data privacy team with responsibility for data protection compliance.

DPIA(s): data privacy impact assessment(s), being tools and assessments used to identify and reduce risks relating to data processing activity. DPIAs can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data. The latest DPIA template will be available from the Data Protection Contact.

EEA: the countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

GDPR: the General Data Protection Regulation ((EU) 2016/679).

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Policy: this internal data protection policy.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the applicable Data Protection Legislation.

Privacy Notices: any and all separate privacy notices, fair processing notices, privacy policies, data promises or similar notices issued or made available by the Company from time to time setting out the Company's Processing activities to Data Subjects. Such notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: the processing of Personal Data as defined in applicable Data Protection Legislation. Broadly this refers to any activity that involves the use of Personal Data, including obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it, and transmitting or transferring it to third parties. If you are in any doubt as to whether your actions constitute the processing of Personal Data you should: (i) contact the Data Protection Contact at hello@sinequanonpictures.com for clarification; and (ii) until such clarification is obtained, assume that your actions constitute the processing of Personal Data.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the Company's privacy or GDPR related policies and guidelines issued from time to time which are related to or referred in this Policy or are otherwise designed to protect Personal Data, including the data retention policy copies of which available from Head of Production on request.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

In this Policy, any words following the terms including, include, in particular, for example, such as or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

Introduction

This Policy sets out how the Company handles the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Policy applies to all Company Personnel ("you" or "your"). You must read, understand and comply with this Policy when Processing Personal Data on our behalf and attend any training on its requirements which is made available to you. This Policy sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this Policy is therefore mandatory and any breach of this Policy may result in disciplinary action.

This Policy may be updated and amended from time to time to take into account new guidance on data protection law and the development of the Company's internal data protection strategy. Related Policies may also be made available to you from time to time. You must also comply with all such updated and amended versions of this Policy and any Related Policies. We will use reasonable endeavours to communicate updates and amendments to this Policy and any Related Policies, you have a responsibility to check for updates to this Policy and any Related Policies before undertaking any new or significant data processing activity.
The terms of this Policy are in addition to, and should be read in conjunction with, any other policies, procedures and guidelines issued by the Company from time to time.
If any provision of this Policy is unclear or you require any further guidance in relation to any particular data processing activity, please contact the Data Protection Contact as soon as possible.
The terms of this Policy (together with Related Policies) are to be treated as confidential information and must not be divulged to any third party without the consent of the Data Protection Contact.

SCOPE

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to EUR 20 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.
All Company Personnel who exercise managerial responsibilities are responsible for ensuring that all Company Personnel who report to them comply with this Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.
The Data Protect Contact is responsible for overseeing this Policy and, as applicable, developing Related Policies. That post is currently held by The Data Protection Contact whose email address is hello@sinequanonpictures.com.
Please contact the Data Protection Contact with any questions about the operation of this Policy or the GDPR or if you have any concerns that this Policy is not being or has not been followed. In particular, you must always contact the Data Protection Contact in the following circumstances:[1]
if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests pursued by the Company) (see paragraph 1);
if you need to rely on Consent and/or need to capture Explicit Consent (see paragraph 2);
if you need to draft Privacy Notices (see paragraph 3);
if you are unsure about the retention period for the Personal Data being Processed (see paragraph 9);
if you are unsure about what security or other measures you need to implement to protect Personal Data (see paragraph 1);
if there has been a Personal Data Breach (see paragraph 2);
if you are unsure whether to, or on what basis to, transfer Personal Data outside the EEA (see paragraph 11);
if you need any assistance dealing with any rights invoked by a Data Subject (see paragraph 12);
whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see paragraph 5) or plan to use Personal Data for purposes others than what it was collected for;
if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making;
if you need help complying with applicable law when carrying out direct marketing activities (see paragraph 6); or
if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (see paragraph 7).

PERSONAL DATA PROTECTION PRINCIPLES
We are responsible for, and must be able to demonstrate compliance with, the data protection principles relating to Processing of Personal Data set out in the GDPR, which require Personal Data to be:

processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
collected only for specified, explicit and legitimate purposes (Purpose Limitation);
adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);
accurate and where necessary kept up to date (Accuracy);
not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);

processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);
not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and
made available to Data Subjects and Data Subjects are allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

LAWFULNESS, FAIRNESS, TRANSPARENCY - LAWFULNESS AND FAIRNESS

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.
You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.
The GDPR allows Processing for specific purposes, the most relevant of which are set out below:
the Data Subject has given his or her Consent (we will usually rely on this lawful basis for marketing communications);
the Processing is necessary for the performance of a contract with the Data Subject (we will usually rely on this lawful basis for fulfilling product orders);
to meet our legal compliance obligations (e.g. if we are required to disclose information by law);
to pursue our or a third party's legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects (the purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices); and/or
to protect the Data Subject's vital interests (e.g. disclosure to paramedics if a person suffers a health emergency on our premises).
Unless the legal ground being relied upon in any given case is recorded elsewhere (e.g. consent was gained and recorded through an online "tickbox" or our contract with the Data Subject (which may include our standard terms of business), you must identify and document the legal ground being relied on for each Processing activity.

CONSENT

As mentioned above, a Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.
A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.
Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented. If you are in any doubt as to whether Consent needs to be refreshed, contact the Data Protection Contact.
It is the Company's policy not to collect or process any personal data which: (i) relates to a child under the age of 13; (ii) are Special Categories of Personal Data; or (iii) are Criminal Convictions Data. In the unlikely event that you do need to process any such data, please contact the Data Protection Contact as soon as possible and prior to doing so. Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Categories of Personal Data and Criminal Convictions Data, for Automated Decision-Making and for cross border data transfers. Where Explicit Consent is required, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.
You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies so that the Company can demonstrate compliance with Consent requirements.

TRANSPARENCY (NOTIFYING DATA SUBJECTS)

The **GDPR** requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Controller, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data. It is the Data Protection Contact's responsibility to ensure that any Privacy Notices that are in place are adequate – however all Company Personnel must ensure that Privacy Notices are made available to Data Subjects prior to any engagement with them that will or may result in the processing of Personal Data.
The Company does not envisage collecting any Personal Data indirectly (for example, from a third party or publicly available source). If you think you need to collect any Personal Data indirectly, please contact the Data Protection Contact first and ensure that you provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

PURPOSE LIMITATION

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.
You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

DATA MINIMISATION

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.
You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.
You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.
You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

ACCURACY

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.
In performing your duties, you will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data you collect at the point of collection and, where applicable, at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

STORAGE LIMITATION

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.
You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.
The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with the Company's guidelines on data retention.
You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable guidelines on data retention.
We must ensure that Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

SECURITY INTEGRITY AND CONFIDENTIALITY - PROTECTING PERSONAL DATA

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. In order to achieve this, you are expected to (among other things):
ensure appropriate protection of files that contain Personal Data sent electronically (internally or externally). For example, for files sent by email, password protect the attachment(s) and send the password in a separate communication. For files on external devices, encrypt those devices and/or password protect the files stored on them and communicate the password to the recipient separately;
ensure the physical security of data by:
adopting a clear desk policy (in accordance with generally accepted good practice and any specific guidelines issued by the Company from time to time) and locking your computer when you are away from your desk – even for a short time;
locking personal data files in adequate storage facilities on-site (e.g. lockable filing cabinets)
ensuring that on-site locations are locked and, if applicable, alarmed, at the end of each day; and
being aware of potential unauthorised visitors to staff-only areas (including by way of persons 'tailgating');
help ensure the digital security of data by:
complying with the instructions, policies and requests of our IT team from time to time relating to digital security;
ensuring that appropriate anti-malware software is running on your computer;
deleting any Personal Data when it is no longer required;
complying with our data recovery policies from time to time in force; and
being wary of (and taking steps to educate yourself about) phishing attacks, social engineering and similar cyber-security threats. If any links or downloadable files look suspect, have them checked out by a member of our IT team;
shred any paper containing Personal Data when no longer required (e.g. because the Personal Data is no longer required, pursuant to the Company's data retention guidelines, or because the data stored on the paper copy has been digitalised);
avoid storing files that contain Personal Data on the local drive of your computer. Files should be stored to a safe remote server (i.e. your team server) with password protection (for confidential files).
We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures (such as those detailed above) against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Criminal Convictions Data from loss and unauthorised access, use or disclosure.
You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.
You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:
Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it. If you exercise a degree of managerial responsibility, it is your responsibility to regularly review access controls relating to your team's access to Personal Data to check that it is appropriate;
Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.
You must comply with, and not attempt to circumvent, the administrative, physical and technical safeguards we implement and maintain in accordance with the applicable Data Protection Legislation and relevant standards to protect Personal Data.

REPORTING A PERSONAL DATA BREACH

The GDPR requires Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Data Protection Contact, and follow the instructions of the Data Protection Contact, who will deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.
You should preserve all evidence relating to the potential Personal Data Breach.
See the UK Information Commissioner's website ico.org.uk for more information.

TRANSFER LIMITATION

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.
You may only transfer Personal Data outside the EEA if one of the following conditions applies:
the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms. At the time of drafting these countries are Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and (where Privacy Shield compliant) the United States, but please check on the EU website for an updated list: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en;
appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Data Protection Contact;
the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

DATA SUBJECT'S RIGHTS AND REQUESTS

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:
withdraw Consent to Processing at any time;
receive certain information about the Data Controller's Processing activities;
request access to their Personal Data that we hold;
prevent our use of their Personal Data for direct marketing purposes;
ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
restrict Processing in specific circumstances;
challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
request a copy of an agreement under which Personal Data is transferred outside of the EEA;
object to decisions based solely on Automated Processing, including profiling (Automated Decision-Making);
prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
make a complaint to the supervisory authority; and
in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.
If you are unsure about the identity of the person purporting to exercise any of the above rights, you must verify the identity of an individual requesting data under any of the rights listed above. Do not allow third parties to persuade you into disclosing Personal Data without proper authorisation.
You must immediately forward any Data Subject request you receive to the Data Protection Contact as soon as possible. The rights specified above are not absolute and the Company will not always be obliged to fulfil Data Subject requests.

ACCOUNTABILITY

The Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.
The Company must have adequate resources and controls in place to ensure and to document GDPR compliance including:
appointing a suitably qualified Data Protection Contact (where necessary) and an executive accountable for data privacy;
implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
integrating data protection into internal documents including this Policy, Related Policies, or Privacy Notices;
regularly training Company Personnel on the applicable Data Protection Legislation, this Policy, Related Policies and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel. If at any time any Company Personnel feels that their training on these subjects is inadequate they should contact the Data Protection Contact as soon as possible; and
regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

RECORD KEEPING

The GDPR requires us to keep full and accurate records of all our data Processing activities.
You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.
These records should include, at a minimum, the name and contact details of the Controller and the Data Protection Contact, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

TRAINING AND AUDIT

We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.
You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.
You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

PRIVACY BY DESIGN AND DPIAs

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.
You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:
the state of the art;
the cost of implementation;
the nature, scope, context and purposes of Processing; and
the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.
The Company must also conduct DPIAs in respect to high risk Processing. Before engaging in any Processing activity which would, or could be, high risk, please contact the Data Protection Contact and request that a DPIA is carried out. You may be required to discuss the findings of that DPIA with the Data Protection Contact. Examples of Processing activity which may be high risk include:
use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

Automated Processing including profiling and Automated Decision-Making;
large scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and
large scale, systematic monitoring of a publicly accessible area.
A DPIA must include:
a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
an assessment of the necessity and proportionality of the Processing in relation to its purpose;
an assessment of the risk to individuals;
the risk mitigation measures in place and demonstration of compliance; and
any other requirements set out in the Company's pro forma DPIA from time to time, which is available from the Data Protection Contact.

DIRECT MARKETING

We are subject to certain rules and privacy laws when marketing to our customers.
For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.
The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.
A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

SHARING PERSONAL DATA

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.
You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.
You may only share the Personal Data we hold with third parties, such as our service providers if:

they have a need to know the information for the purposes of providing the contracted services;
sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
the transfer complies with any applicable cross border transfer restrictions; and
a fully executed written contract is in place setting out how that third party may process the data.

Data Retention Guidance for Sine Qua Non Pictures Limited (the "Company", "we", "our" and "us")

Introduction and scope
This document (the "policy") provides guidance on the Company's policy regarding the retention of personal data. The Company's overriding objective as regards data retention is to ensure that personal data is retained only for as long as is necessary for the purposes for which it is processed (the "Overriding Objective"). Among other things, this will necessitate a case-by-case analysis of factors such as:
our need to perform any agreements between the data subject and us (including order fulfilment);
our need to answer any queries or resolve any problems the data subject may have;
the data subject's continued consent to receive information about the Programme including promotional materials;
our continued provision of our services to the data subject; and

our need to comply with legal requirements (e.g. relating to record keeping).
The Company acknowledges that, in order to fulfil the Overriding Objective, there may be circumstances where personal data may be stored for longer periods or shorter periods than set out in this policy. Accordingly, this policy is intended as guidance only and in the event of any conflict between the Overriding Objective and the terms of this policy, the Overriding Objective shall prevail.
This policy must be read in conjunction with our internal Data Protection Policy and any other documents referred to therein.
This policy does not form part of any employee's contract of employment and we may amend it at any time.
This policy applies to data that is held by third parties on behalf of the Company (for example, cloud storage providers or offsite records storage).
This policy applies to all business units and functions of Sine Qua Non Pictures Limited.
If you have any questions about this policy please contact the Data Protection Contact at hello@sinequanonpictures.com.

ROLES AND RESPONSIBILITIES
Responsibility of all employees and freelancers.
We aim to comply with the laws, rules, and regulations that govern our organisation and with recognised compliance good practices. All employees and freelancers must comply with this policy. Failure to do so may subject us, our employees, and contractors to serious civil and/or criminal liability. An employee's failure to comply with this policy may result in disciplinary sanctions, including suspension or termination. It is therefore the responsibility of everyone to understand and comply with this policy.

TYPES OF DATA AND DATA CLASSIFICATIONS
The Company may retain personal data in the following types of information:

Formal or official records. This may be because we have a legal requirement to retain it, or because we may need it as evidence of our transactions, or because it is important to the running of our business. Please see 1 below for more information on retention periods for this type of data.
Disposable information. Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a formal or official record as defined by this policy. Examples may include:
duplicates of originals that have not been annotated, or paper copies of documents which have been digitised;
preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record;
books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of the Company and retained primarily for reference purposes; and
spam and junk mail.
Please see paragraph 4.2 below for more information on how to determine retention periods for this type of data.

Other personal data. Please refer to paragraph 3.
Confidential information belonging to others. Any confidential information that an employee may have obtained from a source outside of the Company, such as a previous employer, must not, so long as such information remains confidential, be disclosed to or used by us. Unsolicited confidential information submitted to us should be refused, returned to the sender where possible, and deleted, if received via the internet.

RETENTION PERIODS
Subject to the Overriding Principle:

Formal or official records. Any data that is held for legal reasons part should only be retained for the amount of time for it is reasonably required by the business. A record should not be retained longer than is reasonably necessary, unless a valid business reason (or notice to preserve documents for contemplated litigation or other

special situation) calls for its continued retention. By way of example, any personal data collected on Production Start Forms should be deleted and removed from our databases at the end of the particular Production. If you are unsure whether to retain a certain record, contact your line manager and/or the Data Protection Contact at hello@sinequanonpictures.com.
Disposable information. This type of data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of. However, if you are unsure, please contact the Data Protection Contact at hello@sinequanonpictures.com.
Other personal data. As explained above, data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed.

SPECIAL CIRCUMSTANCES

Preservation of documents for contemplated litigation and other special situations. We require all employees to comply fully with our procedures as provided in this policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or the legal department or Data Protection Contact informs you, that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until such person(s) determines those records are no longer needed. Preserving documents includes preserving the integrity of the electronic files or other format in which the records are kept.
If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the Data Protection Contact at hello@sinequanonpictures.com or other relevant compliance manager.

[1] Note: This list is an illustrative examples – but there may be other areas where you want the Data Protection Contact to be consulted or where other business areas have an individual who has expertise in privacy to be able to undertake the tasks set out below in compliance with the GDPR.

For any question don't hesitate to contact us on **hello@sinequanonpictures.com**