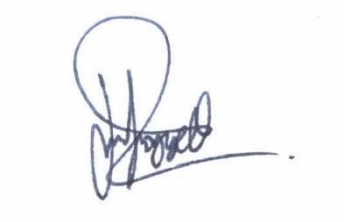
GENERAL DATA PROTECTION REGULATION and INFORMATION & COMMUNICATIONS TECHNOLOGY SECURITY POLICY



Jerry Froggett, Chief Executive Officer
14-04-2020
Reviewed: 01-11-2023

QM-POL-GDPR
GDPR and ICT Security Policy
Version: 005
Issue date: 14-04-2020
Reviewed: 01-11-2023

1 Introduction

Cintra Language Services Group Limited ("Cintra") is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of Cintra Employees, Interpreters, Translators, Board of Directors and Third Parties in relation to the collection, use, retention, transfer, disclosure, and destruction of any Personal Data belonging to a Cintra Contact (i.e., the Data Subject).

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organizations may process Personal Data. An organization that handles Personal Data and makes decisions about its use is known as a Data Controller. Cintra, as a Data Controller, is responsible for ensuring compliance with the General Data Protection Regulation requirements outlined in this policy. Non-compliance may expose Cintra to complaints, regulatory action, fines and/or reputational damage.

Cintra's leadership is fully committed to ensuring continued and effective implementation of this policy, and expects all Cintra Employees, Interpreters, Translators, Board of Directors and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

This policy has been approved by Cintra's Chief Executive Officer, Jerry Froggett.

2 Scope

This policy applies to:

- Cintra Employees, Interpreters and Translators (irrespective of employment status), Board of Directors and Company Secretary.
- Cintra's contractors.

This policy is also applicable to all Cintra's Employees, Interpreters and Translators (irrespective of employment status), Board of Directors and company secretary using Cintra's or others' systems and equipment, whether at Cintra's premises or in their own homes.

- It covers commercially sensitive data and personal data about individuals.
- It is linked to Cintra's Electronic Communications Policy and the Home and Night Worker Policy - Employees.
- Appendix A contains procedures specifically relating to interpreters and translators.

3 Data Protection Principles

3.1 Cintra needs to keep certain information about its employees, interpreters and translators, directors, members, clients, and service users to enable us to carry out our work and monitor performance. It is also necessary to process information so that staff can be recruited and paid, activities organised, and legal obligations fulfilled.

3.2 To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. Cintra must comply with the Data Protection Principles that are set out in the General Data Protection Regulation 2018 (GDPR) which are:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Principle 1: Lawfulness, Fairness and Transparency. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means that Cintra must tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

Principle 2: Purpose Limitation. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means Cintra must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation. Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. This means Cintra must not store any personal data beyond what is strictly required.

Principle 4: Accuracy. Personal data shall be accurate and, kept up to date. This means Cintra must have processes in place for identifying and addressing out-of-date, incorrect, and redundant personal data.

Principle 5: Storage Limitation. Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means Cintra must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

Principle 6: Integrity & Confidentiality. Personal data shall be 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. Cintra must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is always maintained.

Principle 7: Accountability. The Data Controller shall be responsible for and be able to demonstrate compliance. This means Cintra must demonstrate that the six data protection principles (outlined above) are met for all personal data for which it is responsible.

3.3 Computer Security

Cintra regards the integrity of its computer systems as central to the success of the company. Cintra's policy is to take any measures it considers necessary to ensure that all aspects of the systems are fully protected.

4 Responsibilities

4.1 Every Cintra Employee, Interpreter, Translator, Director, contractor, and Company Secretary who processes or uses any personal information or Cintra's electronic systems must ensure that they understand and follow this policy and procedures at all times.

4.2 Confidentiality is crucial in safeguarding Cintra's professional reputation. Every Employee, Interpreter, Translator, Director, contractor, and Company Secretary has the utmost duty to maintain confidentiality at all times.

4.3 New Employees, Interpreters, Translators, Directors, contractors, and Company Secretary will be made aware of the policy and be issued with written instructions on procedures. Reminders will be issued periodically, and training provided where necessary.

4.4 Any Employee, Interpreter, Translator, Director, contractor, and Company Secretary who considers that this policy has not been followed in respect of personal data about him/herself or any other aspect of the policy should raise the matter with the Designated Data Protection Officer. If the matter is not resolved:

- employees should raise it through the grievance procedure
- interpreters and translators should raise it through the raising concerns procedure
- all other personnel should contact a member of the senior management team.

4.5 You have the right to make a complaint at any time to the Information Commissioner`s Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, greatly appreciate the chance to deal with your concerns before approaching the ICO, so please contact us in the first instance.

4.6 Cintra's Chief Executive is responsible for

- ensuring that the organisation and all personnel comply with this policy and the provisions of the General Data Protection Regulation.
- ensuring that appropriate action is taken to resolve any breaches of security or inappropriate use.

4.7 Data Protection by Design

4.7.1 To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

4.7.2 Cintra must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Designated Data Protection Officer, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the Head of Business Operations for review and approval. Where applicable, our external IT department will cooperate with the Designated Data Protection Officer to assess the impact of any new technology uses on the security of Personal Data.

4.8 Compliance monitoring

4.8.1 To confirm that an adequate level of compliance that is being achieved by all Cintra personnel in relation to this policy, the Designated Data Protection Officer will carry out an annual Data Protection compliance audit for each department. Each audit will, as a minimum, assess:

- Compliance with Policy in relation to the protection of Personal Data including:
    - The Assignment of Responsibilities
    - Raising Awareness
    - Training of Employees
- The Effectiveness of Data Protection related operational practices, including:
    - Data Subject Rights
    - Personal Data Transfers
    - Personal Data incident management
    - Personal Data complaints handling
- The Level of understanding of Data Protection policies and Privacy Notices

- The currency of Data Protection policies and Privacy Notices
- The accuracy of Personal Data being stored
- The conformity of Data Processor activities
- The adequacy of procedures for redressing poor compliance and Personal Data Breaches

5 Consequences of breaching the policy

The following final action may be taken by Cintra against those who are found to be in breach of the policy.

- Employees - disciplinary action, including dismissal
- Interpreters and translators – de-registration from Cintra
- Contractors – termination of contract
- Directors – removal from board

6 Notification of data held and processed

6.1 Data Subject Consent

6.1.1 Cintra obtain Personal Data only by lawful and fair means and, where appropriate with the knowledge and Consent of the individual concerned. Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, Cintra is committed to seeking such Consent.

6.1.2 The Designated Data Protection Officer shall establish a system for obtaining and documenting Data Subject Consent for the collection, Processing, and/or transfer of their Personal Data. The system must include provisions for:

- Determining what disclosures should be made in order to obtain valid Consent
- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language
- Ensuring the Consent is freely given (i.e. is not based on a contract that is conditional to the Processing of Personal Data that is unnecessary for the performance of that contract)
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given

- Providing a simple method for a Data Subject to withdraw their Consent at any time

6.3 Data Subject Requests

6.3.1 The Designated Data Protection Officer will establish a system to enable and facilitate the exercise of data subject rights related to:

- Information access
- Objection to processing
- Objection to automated decision-making and profiling
- Restriction of processing
- Data portability
- Data rectification
- Data erasure

6.3.2 If an individual makes a request relating to any of the rights listed above, Cintra will consider each such request in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature. Data subjects are entitled to obtain, based upon a request made in writing/email to hr@cintra.org.uk.

6.3.3 It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

6.3.4 Data Subjects are entitled to obtain, based upon a request made in writing to the Office of Data Protection and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period
- The use of any automated decision-making, including Profiling
- The Right of the Data Subject to:

- Object to Processing of their Personal Data
- Lodge a complaint with the Data Protection Authority
- Request rectification on erasure of their Personal Data
- Request restriction of processing of their Personal Data

6.3.5 If Cintra cannot respond fully to the request within 30 days, the HR Department shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request
- Any information located to date
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision
- An estimated date by which any remaining responses will be provided
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature)
- The name and contact information of the Cintra individual who the Data Subject should contact for follow up

6.4 Law Enforcement Requests & Disclosures

6.4.1 In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of a tax or duty
- By the order of a court or by any rule of law

6.4.2 If a Cintra staff member processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If a Cintra staff member receives a request from a court or any regulatory or law enforcement authority for information relating to a Cintra contact, they must immediately notify the Data Protection Officer who will provide comprehensive guidance and assistance.

6.5 External Privacy Notices

Each external website provided by Cintra will include an online ‘Privacy Notice’ and an online ‘Cookie Notice’ fulfilling the requirements of applicable law.

7 The Data Controller and Designated Data Controllers

7.1 Cintra Language Services Group Ltd. is the Data Controller under the Act, and the organisation is therefore ultimately responsible for implementation and registered with the Information Commissioner`s Office with reference number **Z653803X**. However, Designated Data Controllers will deal with day to day matters.

7.2 Cintra has one Designated Data Controller, who is the **Head of Business Operations** with a number of important responsibilities including:

- monitoring Cintra`s compliance with the GDPR and other data protection laws;
- raising awareness of data protection issues, training Cintra staff and conducting internal audits; and
- cooperating with supervisory authorities such as the ICO on our behalf.

8 Information held

8.1 Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

8.2 Marketing, Training and Profile Data includes your interests and preferences in receiving marketing and training from us, your communication preferences and survey responses.

8.3 We will collect, use, store and process different kinds of personal data about you which we have grouped together follows:

For Interpreters, Translators and Cintra Employees:

- Identity Data includes first name, last name, username or similar identifier, title.

- Contact Data includes home address, corporate or personal email address, telephone and mobile numbers, social media and online accounts such as Skype, Facebook and Twitter.
- Registration Data includes self-employment status, references, qualifications, next of kin, professional memberships, languages, work experience, curriculum vitae, performance, feedback.
- Legal Compliance Data includes passport, national identity card, national insurance number, bank account details, P45 and HMRC starter form, driving licence, work permit, nationality, payroll, pension, health & safety records.
- Special Categories of Personal Data includes security clearances, disability, sexual orientation, relationship status, gender, ethnic background, religion.

For Service Providers and Business Clients:

- Registration Data includes organisation name, registered address, key contact name and job title, business email address and telephone number, website address, invoice recipient and address, company and VAT number.

8.4 If you fail to Provide Personal Data

Where we need to collect personal data by law, or under the terms of a contract or service agreement we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with goods or services). In this case, we may have to cancel a service you have with us but we will notify you if this is the case at the time.

9 Processing of personal information

9.1 Any Employee, Interpreter, Translator, Director, contractor and Company Secretary who processes or uses any personal information is responsible for ensuring that

- Any personal information which they hold is kept securely, and
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Unauthorised disclosure will usually be considered a serious breach of Cintra's rules.

9.2 Personal information should be

- if on paper, kept physically secure when not in use, eg in a locked filing cabinet or drawer.
- If computerised/electronic, kept electronically secure, eg it must be password protected or encrypted.

Cintra employees should not store personal or confidential or irreplaceable Cintra information on the hard drives of office computers, Cintra laptops, Cintra mobile phones (other than telephone numbers) etc or on their own equipment – only Cintra's secure network may be used.

Any item which contains personal information (such as data sticks, laptops, mobile phones, diaries, briefcases etc) should be kept securely when being transported or stored.

Cintra's interpreters and translators must comply with the procedures set out in Appendix A.

9.3 Some personal information is defined as Sensitive Data and needs to be handled with special care. Sensitive Data is defined by the GDPR as that relating to ethnicity, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions. The person about whom this data is being kept must give express consent to the processing of such data, except where the data processing is required by law for employment purposes or to protect the vital interests of the person or third party.

9.4 Sensitive material (personal or confidential data, and/or as defined in 9.3) should be shredded (if in paper format) or fully deleted (if electronic) when no longer operationally required. Particular care should be taken to delete information from computer hard drives/data sticks etc when the data is no longer required or if a machine is to be disposed of or passed on to others.

9.5 Cintra's Employees, Interpreters, Translators, Directors, contractors and the Company Secretary are permitted access only to those parts of Cintra's computer systems which they need in order to carry out their normal duties. Levels of access will be decided by line managers in conjunction with the Designated Data Protection Officer, who will ensure that levels of access are consistent throughout the organisation.

9.6 All Employees, Interpreters, Translators, Directors, contractors and the company secretary must not disclose any personal information or any confidential information obtained via work for Cintra, unless they are required to do so by a senior manager. They are required to sign a Non-Disclosure Agreement with Cintra.

10 Collecting information

10.1 Whenever information is collected about people, they should be informed why the information is being collected, who will be able to access it and to what purposes it will be put. The individual concerned must agree that s/he understands and gives permission for the declared processing to take place, or it must be necessary for the legitimate business of Cintra.

10.2 If personal information is collected by telephone, callers should be advised what that information will be used for and what their rights are under the GDRP.

10.3 Personal or confidential information should preferably not be discussed in public areas of Cintra's work premises or within open-plan office areas, or within public areas of client or service user's premises. All Cintra personnel should be aware of the difficulties of ensuring confidentiality in open-plan or public areas and respect the confidential nature of any information inadvertently overheard.

10.4 Any notes taken during or after an interview should be relevant and appropriate. Notes should be filed in a legible and coherent manner.

10.5 Notes and translation materials should be retained for as short a time as operationally necessary, in a secure place (see 9.2), before being shredded or fully deleted (the exception being any notes taken during criminal investigations which may be taken away during the assignment by the service provider for evidential purposes).

10.6 Papers containing personal and confidential information must be shredded before disposal.

11 Publication

11.1 Cintra aims to make as much information public as is legally possible. In particular, information about Cintra's staff, contractors, interpreters, translators, directors, members, clients and the company secretary will be used in the following circumstances:

- Cintra may obtain, hold, process, use and disclose information in connection with the administration, management and business activities of the company.
- Cintra may publish non-confidential information about Cintra and its staff, directors, members and clients, by means of newsletters, website and other publications.
- Cintra may confirm to any third party whether or not any person is a member or employee of Cintra.
- Cintra may provide approved organisations with lists of names and contact details of members or client organisations only where the members or clients have given their consent or where Cintra is obliged to do so by law.
- Cintra may use information for anything ancillary or incidental to any of the foregoing.
- Names of, and a means of contacting, staff and directors may be published within publicity material and on the website.

- Photographs of key personnel may be displayed at Cintra or placed on the website with their consent.
- Cintra's internal staff and interpreter/translator contact lists will not be treated as public documents and information such as mobile telephone numbers or home contact details will not be given out, unless prior agreement has been secured with the individual concerned.

11.2 Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Designated Data Controller.

11.3 We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract or service agreement we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal or regulatory obligation.

12 How Cintra uses your personal data

12.1 We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data.

Purpose / Activity	Type of data	Lawful Basis for processing including basis of legitimate interest
To register you as a new customer or client	Registration Data	Performance of a service agreement with you
Interpreter and Translator application through our website	Identity Data Contact Data Registration Data	Performance of a service agreement with you
Interpreter and Translator registration	Identity Data Contact Data Registration Data Legal Compliance Data Special Categories of Personal Data	Performance of a service agreement with you Necessary to comply with a legal obligation
Office staff recruitment	Identity Data Contact Data	Performance of a contract with you

	Registration Data Legal Compliance Data Special Categories of Personal Data	Necessary to comply with a legal obligation
Training course application and events	Identity Data Contact Data	Developing new products and services or enhancing existing products and services.
Cintra newsletters and CPD events	Identity Data Contact Data	Necessary for our legitimate interests (for running our business, improve our services and offer training)
Interpreting and Translation assignments	Identity Data	Performance of a service agreement with you
Asking you to leave a review or take a survey	Identity Data Contact Data	Necessary for our legitimate interests (to keep our records updated and to study how customers and linguists use our services)
Marketing, data analytics, customer relationships and experiences	Identity Data Contact Data	Necessary for our legitimate interests (to develop our services and grow our business, for running our business, inform our marketing strategy, to define types of customers for our services and keep our website updated and relevant)

12.2 Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising. You can always control your contact and marketing preferences by updating your preferences or contacting Cintra. You can also opt out from future marketing, advertising and newsletter messages by following the “Unsubscribe” links on any message sent to you.

12.3 Change of purpose

12.3.1 We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

12.3.2 If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

12.3.3 Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

13 Data Processing Partners

13.1 We will disclose the data we collect from you to certain third parties who use personal data in delivering their services to us, they use data securely and confidentially and under strict contractual controls in accordance with data protection laws and enforced by Cintra. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

13.2 We send personal data to the following sets of data processors in order to perform our services:

- Frontier Software, payroll company supervising our payment and payroll activities
- Mailchimp, cloud-based mass email distribution platform
- SurveyMonkey, cloud-based survey, questionnaire and analytical platform
- NEST, auto enrollment compliant pension provider
- The Pensions Trust, pension provider
- Prudential, pension provider
- UKCRB, security clearance provider for Enhanced DBS clearances
- Warwickshire Police, security clearance provider for NPPV3 clearances
- TBW linguist portal, Ministry of Justice interpreting and translation assignments
- Analytics providers, we use analytics and search engine providers that assist us in the improvement and optimisation of our site

13.3 We may also disclose your personal information in the following circumstances:

- If Cintra or substantially all of its assets are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets
- If we are under a duty to disclose or share your personal data in order to comply with any legal or regulatory obligation on request

- Enforce or apply the General Terms of Service and/or the Business Terms and/or any other agreements between you and us or to investigate potential breaches
- Protect the rights, property or safety of Cintra, our customers or others

14 International Transfers

14.1 Some of our external data processors are based outside the European Economic Area (**EEA**) so their processing of your personal data will necessarily involve a transfer of data outside the EEA.

14.2 Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by using specific contracts approved by the European Commission which give personal data the same protection it has in Europe (Privacy Shields).

15 Retention of data

15.1 We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. In general, all information about staff, interpreters and translators will be kept for six years after a person leaves the company. Some information will, however, be kept for longer, including information in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

15.2 To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

15.3 In some circumstances you can ask us to delete your data: see “Request erasure of your personal data” in the `Your legal rights section` for further information.

15.4 In some circumstances we may anonymize your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

16 Computer and data security

16.1 We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used, or accessed in an unauthorized way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality. To provide an extra layer of protection we have an external IT company monitoring all data activities.

16.2 We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

16.3 Passwords

16.3.1 Where the technology allows, passwords must be always used and changed every month. Personnel should not select obvious passwords. All passwords must be kept confidential, and not disclosed to others.

16.3.2 When an employee leaves Cintra or moves to a different department, his/her access levels will be reviewed, or the account suspended/deleted as necessary. When an employee is given a temporary password to a higher level of access than s/he normally uses, that password must be cancelled after the individual ceases to need it. The Department Manager along with the Designated Data Protection Officer is responsible for ensuring that this is done.

16.4 Software

16.4.1 The Designated Data Protection Officer will ensure that all Cintra's computer systems have the industry standard levels of firewalls and virus protection.

16.4.2 All software used on Cintra's systems must be formally authorised by the Designated Data Protection Officer and the ICT contractor, as necessary. Compliance will be monitored.

16.4.3 Cintra's Employees, Interpreters, Translators, Directors, contractors, and company secretary who use Cintra's electronic/computer systems must not test or implement any products that may compromise the systems' confidentiality, availability or integrity.

16.4.4 Cintra's Employees, Interpreters, Translators, Directors, contractors, and company must not possess, reproduce or use computer programs for scanning Cintra's networks without prior approval from the Designated Data Protection Officer.

16.4.5 Cintra's employees, contractors, interpreters, translators, directors, and company secretary must not implement/run/download any software or perform any action that could interfere with or jeopardise the integrity of Cintra's computer/electronic systems.

16.5 Systems back-up

In addition to the automatic and off-site back-ups, Department managers are responsible for stipulating requirements for any additional back-up operations in their own departments. Regular back-up must be carried out in accordance with departmental instructions.

16.6 Safekeeping

16.6.1 Disks, data sticks and other mobile storage devices containing confidential information must be stored and transported securely. Passwords and/or encryption should always be used.

16.6.2 Cintra laptops and other electronic equipment belonging to Cintra, or personal equipment containing confidential data, must be stored and transported securely. If using such equipment at home, personnel are expected to take reasonable steps to secure their homes from burglary.

16.6.3 All Employees, Interpreters, Translators, Directors, contractors and Company Secretary must ensure that they do not compromise the physical security of Cintra's office, its contents and all other Cintra equipment. Employees should be aware of and follow building security procedures.

17 Computer systems misuse

17.1 Misuse of computer systems is a serious breach of Cintra's rules. The following are examples of misuse:

- fraud and theft
- system sabotage
- introduction of viruses and time bombs
- using unauthorised software
- obtaining unauthorised access for self or others
- using the system for private work or game playing
- disclosure of passwords to others
- breaches of the Data Protection Act and this policy
- breaches of Cintra's Electronic Communications and Social Media Policy
- hacking

This list is not exhaustive. Depending on the circumstances of each case, misuse of the system may be considered gross misconduct. Alleged misuse may be reported to the police.

17.2 Cintra's management, where necessary in consultation with specialist auditors or other external parties, may institute confidential control techniques and safeguards. Financial systems are subject to special reconciliation processes.

18 Your legal rights

You have rights under The General Data Protection Regulation in relation to your personal data. Please see below to find out more about these rights:

You have the right to:

**Request access to your personal data (commonly known as a "data subject access request"). ** This enables you to receive a copy of the personal data we hold about you. If you require this, then please contact our HR department.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though

we may need to verify the accuracy of the new data you provide to us. If you require this, then please contact our HR department.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request. This information could be related to pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. Cintra is under certain obligations to retain certain data for a minimum of 6 years. Please note that these retention requirements supersede any right to erasure requests under applicable data protection laws.

Object to processing of your personal data. This is in situations where we are relying on a legitimate interest (or those of a third party) and there is something about your situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights. Cintra is under certain obligations to process and retain certain data for compliance purposes. Please note that these requirements supersede any right to objection requests under applicable data protection laws. If you object to the processing of certain data, then we may not be able to provide the Cintra Services or maintain our service level agreement and it is likely we will have to terminate your account.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it. Please note that any requests in relation to the restriction of the processing of your data means that we may not be able to perform the contract we have or are trying to enter with you. In this case, we may have to cancel your use of our services or your service level agreement with us, but we will notify you if this is the case at the time.

Request the transfer of your personal data to you or to a third party. We will provide to you, your personal data in a structured, commonly used, machine-readable format, which you can then transfer to an applicable third party. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you. If you require this then please reach out to our HR Department.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide the Cintra Services to you or maintain the service level agreement. We will advise you if this is the case at the time you withdraw your consent.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made several requests. In this case, we will notify you and keep you updated.

Appendix A

Data protection and information electronic security procedures for Cintra's interpreters and translators

These procedures give some practical ways in which you can comply with Cintra's General Data Protection Regulation and Information & Communications Technology Security policy, which you are required to implement.

Please also ensure you read and comply with the full policy.

Protecting confidential information that you hold electronically about Cintra clients is vitally important. This applies equally to emails relating to assignments as well as to translated documents.

In practical terms this means that you MUST:

- Have an up-to-date firewall and anti-virus system on your PC, laptop and hard drive.
- If you use your PC, laptop, external hard drive, cloud storage media or mobile phone for Cintra work, have secure and robust passwords. Change your passwords every month. Ensure that only you can access your Cintra work.
- If you use memory sticks for Cintra work, then only encrypt able sticks may be used.
- Do not store confidential material arising from Cintra assignments on a memory stick or other mobile electronic storage media without Cintra's permission. If you are required to use this method of storage, then the memory stick or CD, for example, must be kept in a secure place and all individual documents must be password protected.
- Password protect **every** file containing Cintra material arising from assignments.
- Never leave passwords lying around.
- Never leave your laptop in an insecure place (including in your car or your kitchen table).
- Take adequate precautions to protect your home/office from burglary.
- Only keep confidential files or emails if necessary, for example a witness statement should be destroyed once you are confident it is safely in the hands of the police officer concerned. In normal circumstances, witness statements should not be kept by you longer than 3 days.
- When you delete files containing confidential material, ensure that you delete them fully.

- Witness statements can only be translated at the police station. If an officer insists on completing the statement at home, then the officer must call Cintra to give approval to the interpreter.
- **DO NOT**, under any circumstances, email witness statements from your own email address either to Cintra or to a police force. If post is used, it must be **special delivery** and Cintra needs to be told the tracking number. Keep the receipt and the tracking slip (showing the bar code). If you are asked to deliver the translation by hand, please provide the name of the officer who requested this. Tell us the name of the person you handed the envelope to, or if you left it at the reception desk.
- Any other documents or electronic storage media (eg CDs) should be posted by registered 'signed for' post or special delivery, as agreed with the Translations Team on each occasion. Standard postage should never be used.
- Remember that personal email traffic is NOT secure. If the customer requires that a confidential document be emailed in a secure manner you will not be able to do this by using your own email address. Instead, the document must be emailed from Cintra's special secure email to a customer's secure email. Contact the Cintra's Translations Team for more information about this.
- For Cintra communication, have a confidential email that only you in your household can access.
- Inform Cintra immediately if you think your electronic security has been compromised (e.g., your email has been hacked or your laptop containing confidential Cintra material arising from assignments has been stolen).
- Securely store and transport papers and diaries containing confidential information. Keep the information only if it is operationally needed and always shred prior to disposal. For example, keep Cintra work in a locked filing cabinet when not in use.

For Video Calls (Skype etc.)

- Ensure that your environment is private, noise and distraction free.
- Confidentiality remains of paramount importance, as with all assignments. It is preferable that video calls are made in separate rooms away from other members of your household.

- Please try to ensure that your ‘background’ (what can be seen by your device video camera behind and around you) are clean, tidy and professional. It is preferable to have a clear background such as a blank wall with any artwork or photographs removed to avoid distractions for service users.
- Do not allow any interruptions to the video call, e.g., to take other calls on another phone, answer the doorbell or speak with others.
- Try to avoid using the speakerphone. It is highly preferable to use headphones for all Skype video calls to maintain confidentiality.
- Ensure that your internet connection is adequate for the video call. Preferably, please prioritise using your home broadband and Wi-Fi internet connection over your mobile phone network.
- All documents, including witness statements and notes created during the video session should be securely destroyed once you are confident that they are safely in the hands of the police officer concerned.
- The video conference call should not be recorded or copied unless by the designated Constabulary Image technicians or authorised personnel.