eurocom ci

T: 01372 886 920
F: 01372 351 219
info@eurocomci.co.uk
Granary House, 18a North Street
Leatherhead, Surrey, KT22 7AW

EUROCOM CI LTD

GDPR DATA PROTRECTION POLICY

Implementation date: 25th May 2018

## 1. Introduction

Eurocom CI Ltd is committed to operate in accordance with all applicable data protection laws regulations and in line with the highest standards of ethical conduct. This document sets out the expected behavior of employees and third parties (if applicable) of Eurocom CI Ltd in relation to **processing** of any **personal data** belonging to their Data Subjects. Eurocom CI Ltd, as a Data Controller and Data Processor, is responsible for ensuring compliance with the data protection requirements outlined in this policy.

## 2. Definitions

**'Employee'** is an individual who works part-time or full-time for Eurocom CI Ltd under a contract of employment, whether oral or written, express or implied, and has recognized rights and duties. Includes temporary employees and independent contractors.

**'Third Party'** is an external organisation that conducts business with Eurocom CI Ltd and is also authorised by Eurocom CI Ltd to process personal data of Eurocom CI Ltd.

'**Personal data'** means any information relating to an identified or identifiable living natural person ('data subject'); an identifiable living natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**'Sensitive personal data'** means personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c ) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

'**Processing**' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording,


Co Registration No. 02387512 | VAT No 890 0227 39 | Data Protection : Z9753599

organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**'Data Subjects'** Data subject means an individual who is the subject of personal data. In other words, the data subject is the individual whom particular personal data is about.

**'Data Controller'** means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are to be, processed.

**'Data Processor'** in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

## 3. Application.

Eurocom CI Ltd has set comprehensive but proportionate governance measures, management support and direction for data protection compliance in a framework of policies and procedures. Our business monitors compliance with data protection policies and regularly reviews the effectiveness of data handling / processing activities and security controls. Our business has developed and implemented a needs-based data protection training program for all staff, appropriate technical and organisational measures that ensure and demonstrate that we comply. Measures include data protection policies, staff training and internal audits of processing activities and compliance with Cyber Essentials and IASME certification.

Our business has documented the personal data we hold, where that data came from and who it is shared with. Eurocom CI Ltd conducted an information audit across the organisation to map data flows and document the lawful basis of processing.

**4. Data Protection by Design and Data Protection Impact Assessments**. Our business has implemented appropriate technical and organisational measures which show we have considered and integrated data protection into our processing activities. Our business understands when we must conduct a data protection impact assessment (DPIA). The processes to action this is at Annex A. DPIAs are a tool which help identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy. The DPIA allows us to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

**5. Data Protection Officers**. Eurocom CI Ltd has designated responsibility for data protection compliance to a suitable individual within the organisation. An external organisation is being sought to be appointed as Data Protection Officer (DPO).

**6. Lawful basis for processing personal data**.

**Article 6(1)** of the GDPR sets out the conditions the must be met for the processing of personal data to be lawful. The conditions, which Eurocom CI Ltd adheres to, are:

i. The data subject has given consent to the processing of their personal data for one or more specific purposes.

ii. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

iii. Processing is necessary for compliance with a legal obligation to which the controller is subject.

iv. Processing is necessary in order to protect the vital interests of the data subject;

v. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

vi. Processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. These conditions are all equally valid and Eurocom CI Limited assesses which of these grounds are most appropriate for different processing activities and then fulfil any further requirements the GDPR sets out for these conditions (GDPR Article 5). Processing activities that fall under performance of a contract, legal obligation, vital interests and public task may be fairly straight-forward to identify. The key is assessing whether Consent or Legitimate Interests will be most appropriate for specific processing of personal information

**7.** ***Consent. As a legal grounds for processing personal data.***

a. **Definition**. GDPR defines Consent in Article 4(11) as: 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. It should be noted that our business does not offer services directly to children.

b. **Giving Consent.** Our business has reviewed how we seek, record and manage consent and the systems currently used to record consent implemented appropriate mechanisms to ensure an effective audit trail. Consent requires a positive opt-in and should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting the website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided. It should be noted that Eurocom CI Limited:

i. Does not use pre-ticked boxes or any other method of consent by default.

ii. Requires consent to be named, i.e. third parties with whom the data may be shared will, where possible be specifically named. Simply providing categories of third parties will not be acceptable.

iii. Aims to ensure consent is granular, i.e. separate consent is obtained for independent processing operations.

iv. Ensures consent isn't a pre-condition to receive our services but for website registration agreement with our data protection policy is required. It does not bundle it in with Terms & Conditions.

v. Ensures consent is only be relied upon if; there is no other lawful basis for processing; we can give individuals a genuine choice or when we are required to have consent

vi. If the data subjects wish to remove consent then they can do so by sending an email to info@eurocomci.co.uk

c. **Other Legitimate Interests**. There are other legitimate interests as a legal ground for processing personal information. The ICO has set up a Working Party, to produce guidance for commercial and not-for-profit organisations on the use of Legitimate Interests under the General Data Protection Regulation (GDPR). The ICO's draft guidance on Consent states: 'consent is one lawful basis for processing, but there are five others. Consent won't always be the easiest or most appropriate'. When considering whether you can rely on Legitimate Interests, Eurocom CI Limited uses four key factors:

i. It will be necessary to demonstrate that Eurocom CI Limited has balanced its interests with the interests and rights of the individuals affected by your proposed processing activity.

ii. The assessment, which may be a simple process or very detailed in more complex scenarios, will be documented as it may be challenged by individuals or the Regulator.

iii. Eurocom CI Limited will inform individuals that we are processing their personal information under this condition (i.e. via our Privacy Policy).

iv. Eurocom CI Limited will need to be able to uphold the individual's right to object to such processing.

v. Recital 47 of the GDPR broadly describes areas where Legitimate Interest might be relied upon*, for example when the processing is strictly necessary for the purposes of preventing fraud or ensuring network security, where there is a 'reasonable expectation' or a 'relevant and appropriate relationship'. Recital 47 also specifically mentions; 'the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate purposes'.*

**8. Communicating privacy information**. Our business has reviewed our current privacy notices and has a plan in place to make any necessary changes in time for GDPR implementation, including the need to explain the legal basis for holding information.

**9. Individuals' rights**. Our business has checked our procedures to ensure that we can deliver the rights of individuals under the GDPR.

**10. Subject access**. Our business has reviewed our procedures and has plans in place for how we will handle requests from individuals for access to their personal data within the new timescales outlined in the GDPR. Annex C

**11. Breach notification.** Eurocom CI Limited has implemented appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively. Our business has mechanisms in place to assess and then report relevant breaches to the ICO where the individual is likely to suffer some form of damage e.g. through identity theft or confidentiality breach. This includes a mechanism to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms.

**12. Transfer of data.** Our business operates in the UK and the UK ICO is the lead supervisory authority.

Annexes:

A. **Process For Data Protection Impact Assessments**
B. **Data protection, privacy and communications policy**

Annex A.

**Process For Data Protection Impact Assessments**.

1. Our business understands when we must conduct a data protection impact assessment (DPIA): a tool which can help identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy. An effective DPIA allows us to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. We have carried out an initial DPIA , we do not currently believe we have a problem. We will, however, undertake a DPIA in cases where it is unclear whether doing so is required. It will contain the following information:

    1.1. A description of the processing operations and the purposes including, where applicable, the legitimate interests pursued by the controller.

    1.2. An assessment of the necessity and proportionality of the processing in relation to the purpose.

    1.3. An assessment of the risks to individuals. The measures in place to address risk, including security and to demonstrate that you comply.

2. A DPIA can address multiple processing operations that are similar in terms of the risks presented, providing adequate consideration is given to the specific nature, scope, context and purposes of the processing. If the processing is wholly or partly performed by a data processor, then that processor will assist in carrying out the DPIA. It may also be appropriate to seek the views of data subjects in certain circumstances.

**Annex B**

**Data protection, privacy and communications policy.**

**1. Introduction.** The Company holds personal data about job applicants, employees, beneficiaries, partners, clients, customers and other individuals for a variety of purposes connected with the Company's work. This policy sets out how the Company seeks to protect personal data and ensure staff understand the rules governing their use of personal data to which they have access in the course of their work. This policy requires staff to ensure that the Managing Director should be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed. The main point of contact for all Data Protection issues is the Managing Director, Jagriti Patwari.

**2. Scope.** This policy applies to all staff, which for these purposes includes employees, temporary and agency workers, other contractors and interns. All staff must be familiar with this policy and comply with its terms. The Company may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

**3. Definitions.** In this policy:

**3.1. Business purposes** means the purposes for which personal data may be used by the Company, e.g. personnel, administrative, financial, regulatory, payroll and employee screening purposes;

**3.2. Personal Data** means information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, interns, clients, customers, candidates and suppliers. This includes expression of opinion about the individual and any indication of someone else's intentions towards the individual.

**3.3. Sensitive Personal Data.** Means personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, sexual life, criminal offences, or related proceedings. Any use of sensitive personal data must be strictly controlled in accordance with this policy.

**3.4. Processing Data.** Means obtaining, recording, holding or doing anything with it, such as organising, using, altering, retrieving, disclosing or deleting it.

**4. General principles.** The Company's policy is to process personal data in accordance with the applicable data protection laws and rights of individuals as set out in this policy. All employees have personal responsibility for the practical application of the Company's data protection policy. The Company will observe the following principles in respect of the processing of personal data:

**4.1.** to process personal data fairly and lawfully in line with individuals' rights;

**4.2.** to make sure that any personal data processed for a specific purpose are adequate, relevant and not excessive for that purpose;

**4.3.** to keep personal data accurate and up to date;

**4.4.** to keep personal data for no longer than is necessary;

**4.5.** to keep personal data secure against loss or misuse;

**4.6.** not to transfer personal data outside the EEA (which includes the EU countries, Norway, Iceland and Liechtenstein) without adequate protection.

**5. Fair and lawful processing.** Staff should not process personal data unless:

**5.1.** the individual whose details are being processed has consented to this;

**5.2.** the processing is necessary to perform the Company's contractual or legal obligations or exercise legal rights;

**5.3.** the processing is otherwise in the Company's legitimate interests and does not unduly prejudice the individual's privacy;

6. **Gathering Data**. When gathering personal data or establishing new data protection activities, staff should ensure that individuals whose data is being processed receive appropriate data protection notices to inform them how the data will be used. There are limited exceptions to this notice requirement. In any case of uncertainty as to whether a notification should be given, staff should contact the Managing Director. For each piece of personal information and special category data we hold, we identify whether we are the controller or processor, and record the purpose and justification for which it was obtained.

**7. Sensitive Data**. It will normally be necessary to have an individual's explicit consent to process 'sensitive personal data', unless exceptional circumstances apply or the processing is necessary to comply with a legal requirement. The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact the Managing Director for more information on obtaining consent to process sensitive personal data.

8. **Data classification** Data is classified as Red: Highly sensitive, Amber: Confidential, Green: Public. All data we hold are in the red and amber category. Sensitive data will be identified from the information provided by candidates on the online DBS checks system and Xavier. These will be treated differently to other data by way of not disclosing any information in relation to it over the phone, it will only be disclosed in writing to the HR professionals with the right to know as part of the service we provide and when dealing with subject access requests.

**9. Accuracy, adequacy, relevance and proportionality.** Staff should make sure data processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

**9.1.** Individuals may ask the Company to correct personal data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and process followed as per Annex C.

**9.2.** Staff must ensure that personal data held by the Company relating to them is accurate and updated as required. If personal details or circumstances change, staff should inform the Company so the Company's records can be updated.

**9.3.** Individuals may ask the Company to delete or suspend the processing of their records. Process in relation to this is set out in Annex C

**10. Security.** Staff must keep personal data secure against loss or misuse. Where the Company uses external organisations to process personal data on its behalf additional security

arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. Staff should consult the Managing Director to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement.

11. **Data retention.** Personal data should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances including the reasons why the personal data were obtained. We will be responsible for keeping data of completed screenings and DBS checks for 6 months after the date of completion of the work, after which all data will be archived. Where we have started to collect data for screenings or DBS checks from candidates, however the screening was never completed, the data we hold will be available for 6 months from the date that the candidate was added to our systems, after which the data will be archived. All data will be deleted after 6 years.

12. **Rights of individuals.** Individuals are entitled (subject to certain exceptions) to request access to information held about them. All such requests should be referred immediately to the Managing Director per Annex C. This is particularly important because the Company must respond to a valid request within the legally prescribed time limits.

13. **Reporting breaches.** Staff have an obligation to report actual or potential data protection compliance failures to the Managing Director. This allows the Company to:

13.1. Investigate the failure and take remedial steps if necessary.

13.2. Make any applicable notifications.

14. **Consequences of failing to comply.** The Company takes compliance with this policy very seriously. Failure to comply puts both staff and the Company at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

15. **Website Statement.**

15.1. Eurocom CI Limited is committed to protecting individuals' privacy. This policy describes how Eurocom CI Limited collects and uses personal information about people who visit our websites and give us their data over the phone, face to face, and in writing. The terms of this policy may change, so please check it from time to time. If you have any queries about this policy please contact: Eurocom CI Limited, 18a North Street, Leatherhead, Surrey, KT22 7AW. Eurocom CI Limited is registered under the Data Protection Act 1998, registration no. Z9753599 and is preparing to meet the requirements of General Data Protection Regulation (GDPR), which will be introduced in May 2018.

15.2. **How do we collect information?** We may collect personal information from a variety of sources, including from individuals, their new employers, previous employers, educational establishments, professional bodies, credit agencies, character referees, Police National Database, Companies House, UK Border Agency. We collect personal information when individuals register with us as a user of the portal, as a client or candidate, participate in our events or when individuals communicate with us by e-mail, telephone or in writing. When the Company collects personal data from a subject, we clearly state what it is being collected for, how it will be processed and who will process it, and if the data subject is required to provide consent for that processing activity

15.3. **What information do we collect?** In general, the personal information we collect includes (but is not limited to): name, contact details (including phone numbers and

electronic and postal addresses), and organisational and employment details where an individual is a member of staff or otherwise linked to an organisation. We collect all information that may be required to conduct a pre employment screening including, but not limited to, date of birth, national insurance number, 10 year residential address history, credit history, 10 year previous employment history, character referees, criminal history, directorship history, identity documentation, education history and professional qualifications and membership records. We also collect information that is not personal information. For example, we may collect information relating to an individual's passport details pre employment checking notes on communications with various sources. We generally use this information in order to be able to fulfil our contractual obligation to clients in conducting pre employment screening and DBS checks in order that our clients can make appropriate hiring decisions

15.4. **Transfer of data outside the EEA** There are employees who may have had education, qualifications and employments outside the EEA for which clients and candidates have asked us to get references. We will request explicit consent from candidates in relation to requesting confirmation of education and professional qualification and employments that are outside the EEA. It is in the candidate's interest to have these references for their potential employer and we will be writing to non EEA countries with the name of the candidate and one other piece of personal identifiable information for them to provide us with a reference. .

15.5. **How do we use this information?** We will use an individual's personal information for:

15.5.1. Conducting the pre employment checks that has been agreed in the service level agreement of clients;

15.5.2. Reporting to clients on the results of the checks undertaken;

15.5.3. Requesting feedback on the level of service provided;

15.5.4. Conducting anti money laundering checks on individuals who have access to our eBulk and Xavier platform to undertake checks on employees;

15.5.5. For billing our services rendered to our clients;

15.5.6. Administering screenings and checks relating to our suppliers or customers;

15.5.7. Inviting clients to events, webinars and communicating with clients and candidates as necessary to competently provide the services we have been contracted to undertake;

15.5.8. For administrative purposes;

15.6. **Eurocom CI Limited's Privacy Statement.** The Data Protection Act 1998 and GDPR provide the legal framework that defines how personal information can be used. Eurocom CI LImited is fully committed to complying with the Data Protection Act 1998 and has a legal duty to protect any information we collect.

15.6.1. Personal information is only used for the purpose for which we collect it.

15.6.2. Only information that we actually need is collected.

15.6.3. Relevant Personal information is only seen by those who need it to do their jobs, for example passport details to employee screeners etc.

15.6.4. We will not pass an individual's personal information on to any other organisation without the individual's consent unless we are required to do so by law.

15.6.5. Personal information is retained only for as long as it is required for the purpose collected.

15.6.6. We will, where necessary, keep individuals' personal information up to date.

15.6.7. Personal information will be protected from unauthorised or accidental disclosure.

15.6.8. We will provide individuals with a copy of their personal information on request.

15.6.9. Inaccurate or misleading data will be corrected as soon as possible.

15.6.10. These principles apply whether we hold individuals' personal information on paper or in electronic form.

15.7. **Access Rights and Requests.** The data subject has the right to see what personal data we hold about them and where appropriate in a machine readable format, they have a right to correct inaccurate records, delete records and suspend the processing of records. Subject access requests must be submitted in writing. Should the data subject wish to obtain a copy of the personal information we hold about them, a request should be submitted to: Eurocom CI Ltd, Granary House, 18a North Street, Leatherhead, Surrey, KT22 7AW; info@eurocomci.co.uk

15.8. **How do we protect personal information?** Other than in relation to Non-Confidential Information, we will take all reasonable steps to protect the personal information that we hold from misuse, loss, or unauthorised access, including by means of firewalls, password access, secure servers and encryption of financial transactions. We take appropriate measures to ensure that the personal information disclosed to us is kept secure, accurate, and up to date. We will ensure that individuals' personal information is kept only for so long as is necessary for the purposes for which it was collected and is securely destroyed in accordance with our data retention and disposal policy.

15.9. **Will we disclose the information we collect to outside parties?** We will only disclose data when obliged to disclose personal data by law, or the disclosure is 'necessary' for purposes of national security, taxation and criminal investigation, or we have the individual's consent.

15.10. For every contract we hold with suppliers and customers involving the processing of personal data the Company will confirm whether we are the data controller or data processor

15.11. Where personal data is disclosed to a supplier/provider that the contract with them explicitly imposes the obligation to maintain appropriate technical and organisational measures to protect personal data in line with relevant legislation

15.12. Where data storage, applications or other services are provided by another business (such as a cloud provider Office 365, google cloud etc), there is independently audited,

written confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those used by Eurocom CI Ltd.

Annex C

Subject Access and Data Portability

When a subject access request is received, there will be identity verification on the individual requesting access to ensure that it is a legitimate request. Identity verification will mean checking our systems to ensure that the contact details we hold are the same contact details that the subject access request is coming from. This identity verification can be undertaken by any staff dealing with customer requests.

Once the identity is verified, Jagriti Patwari and Orsi Mihaly will be notified of the subject access request

Responsibilities of Orsi Mihaly and Jagriti Patwari

- Determine whether there are any other processors or controllers that need to be notified of the subject access request
- Notify any other processors or controllers that are deemed to be necessary
- Provide all personal data that we hold or process that belongs to the subject
- If data has been request in a machine readable format then liaise with the subject to determine the best format to provide the data that will be helpful to them

Correcting inaccurate records, deleting records and suspending processing of records

When a subject access request is received, there will be identity verification on the individual requesting correction/deletion/suspension to ensure that it is a legitimate request. Identity verification will mean checking our systems to ensure that the contact details we hold are the same contact details that the subject access request is coming from. This identity verification can be undertaken by any staff dealing with customer requests.

Once the identity is verified, Jagriti Patwari and Orsi Mihaly will be notified of the data subject request

Responsibilities of Orsi Mihaly and Jagriti Patwari

- Determine whether there are any other processors or controllers that need to be notified of the data subject request
- Notify any other processors or controllers that are deemed to be necessary
- Determine whether the data needs to be corrected and if it is determined that correction is not necessary then note the request was made and document the reasons for not making the change
- Where deletion is deemed correct then the following locations of data will need to be deleted; server files, Xavier, Machform, DBS checks website, emails
- Where suspension is deemed necessary then the data subject's screening or DBS check will be put on hold according to instructions received by the data subject