The EU Data Privacy Standards (the "Standards")

1. PURPOSE

1.1 **About us**: Flex is a socially responsible and leading electronics manufacturing services provider delivering design, engineering and manufacturing services to aerospace and defense, automotive, computing, consumer, industrial, infrastructure, medical, energy and mobile original equipment manufacturers. Flex helps customers design, build, ship and service electronics and other products through a network of international facilities. This global presence provides design and engineering solutions combined with core electronics manufacturing and logistics services.

1.2 **Our commitment to data privacy**: These Standards set out our approach to and the commitment of the Flex Group and its Executive Management and Board of Directors to maintaining the highest standards of data privacy. These Standards for processing of Personal Data relate to the Personal Data of employees, contractors and business contacts or other individuals and must be followed by all members and employees of the Flex Group, and the Executive Management and Board of Directors will enforce such compliance. Failure to comply with these Standards, will lead to appropriate corrective and disciplinary actions.

1.3 **Objective of these Standards**: We shall handle all Personal Data in accordance with Data Protection Laws and all other Applicable Law. Our compliance with these Standards will provide you with the protection required to enable us to process certain Personal Data within the Flex Group, including the transfer of that Personal Data outside of the EEA.

2. DEFINITIONS AND ABBREVIATIONS

Applicable Law means all applicable local data protection and privacy laws and regulations including, but not limited to, the Data Protection Laws.

Business Contact Data means Personal Data relating to *the business contacts at Flex Group's customers and suppliers;*

Data Controller means the natural or legal person who alone or jointly with others determines the purposes and means of processing Personal Data;

Data Privacy means data protection as promulgated by Data Protection Laws;

Data Processor means the natural or legal person which processes Personal Data on behalf of the Data Controller;

Data Protection Laws means, where applicable:

(a) the following laws:

(i) the Regulation;

(ii) the European Privacy and Electronic Communications Directive (Directive 2002/58/EC),

including as implemented or promulgated in EEA member states each as amended, supplemented, substituted or replaced from time to time.

Data Subject means an identified or identifiable natural person;

EEA means the European Economic Area which comprises the countries of the European Union plus Iceland, Liechtenstein and Norway;

Employee Personal Data means *Personal Data relating to: (a) current, former and prospective employees; (b) current, former and prospective individual contractors; (c) volunteers; (d) agents; (e) temporary and casual workers; and (f) dependants, relatives, guardians and associates of the Data Subjects set out in (a) to (e) of the Flex Group;*

Flex Group means Flex Ltd. incorporated in Singapore and located at 2 Changi South Lane, Singapore and any of its subsidiaries bound by these Standards;

Global Data Privacy Officer shall be the Data Protection Officer as defined by the Regulation;

Global Data Subject Rights Policy means the policy attached under **Annex C** of these Standards;

Global Procedure for Raising and Handling Data Privacy Complaints means the policy attached under **Annex D** of these Standards;

Personal Data means any information relating to an identified or identifiable natural person who can be identified directly or indirectly from that information, including but not limited to Employee Personal Data, Business Contact Data and Third Party Data;

Regulation / GDPR means the General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and any law which implements, supplements, relates to or replaces it.

Processing shall have the meaning set out in Article 4(2) of the Regulation and **process** and **processes** shall be construed accordingly.

Special Category Data means any Personal Data revealing a Data Subject's racial or ethical origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data processed for the purposes of uniquely identifying a natural person; data about health, sex life or sexual orientation and shall for the purposes of these Standards include data relating to criminal convictions and offences;

Supervisory Authority means any competent data protection or privacy authority.

Standards means the terms set out in this document;

Third Party Data means Personal Data relating to third parties such as contact details about other individuals, information about complaints and CCTV images;

we, our and/or us means the Flex Group and its employees; and

you means a Data Subject whose Personal Data is processed by the Flex Group.

3. BACKGROUND

3.1 What is Data Privacy law?

Data Privacy (also known as "data protection") requires companies to process Personal Data in accordance with certain good practice principles. It also grants certain rights to individuals (for example, to access and correct their information). Data Privacy law governs the way in which Flex collects, stores and uses Personal Data about employees, contractors, business contacts and other individuals.

3.2 How does Data Privacy law impact Flex internationally?

Data Protection Laws (in particular, the restrictions set out in the GDPR on the transfer of Personal Data outside of the EEA in order to ensure that the level of protection of Data Subjects is not undermined) do not permit the international transfer of Personal Data to countries outside the EEA unless they ensure an adequate level of data privacy. Flex has taken proper steps to ensure that any transfer of Personal Data to countries outside the EEA is lawful. These Standards create a binding corporate rules framework to comply with rules contained in the Data Protection Laws and provide an adequate level of protection for Personal Data transferred to Flex Group companies outside the EEA , in particular in accordance with Data Protection Laws (in particular the mechanism set out in the GDPR for the approval of binding corporate rules). Flextronics International Gesellschaft m.b.H d is the member of the Flex

Group with delegated Data Privacy responsibilities and will be responsible for compliance with these Standards in this context.

4. SCOPE

4.1 **Data covered by these Standards:** These Standards apply to our processing and the transfer by us of Personal Data which is subject to the Data Protection Laws for which we are a Data Controller and to:

(a) the processing of this Personal Data by a member of the Flex Group within the EEA;

(b) the processing of this Personal Data in the EEA by a member of the Flex Group located outside the EEA;

(c) the transfer of this Personal Data from within the EEA to outside the EEA by a member of the Flex Group to another member of the Flex Group and the subsequent processing or onward transfer of this Personal Data by that member to other members of the Flex Group.

(d) The processing we carry out may be manual or automated. The types of Personal Data which are processed by us are Employee Personal Data, Business Contact Data and other Personal Data.

4.2 The tables appended at **Annex B** of these Standards contain a general description of the Personal Data which is undergoing the transfers under these Standards.

4.3 The Standards apply to all processing of Personal Data within the Flex Group where such Personal Data are subject to the Data Protection Laws and Paragraph 4.1 of the Standards.

5. PRINCIPLES

Where Flex is a Data Controller, the following principles shall apply:

5.1 **We process Personal Data lawfully, fairly and in a transparent manner ("lawfulness, fairness and transparency"):** We will process Personal Data fairly and lawfully. One or more of the conditions set out in **Annex A** or under Data Protection Laws, which should be relied on in order to legitimise data processing, will always be met. We will make sure that it is clear to you how Personal Data concerning you are collected, used, consulted or otherwise processed and to what extent the Personal Data are or will be processed. We will also provide information as required by Data Protection Laws including information to explain how we may disclose and/or transfer Personal Data as well as the legal basis for Processing, legitimate interests, categories of recipients and available rights. Any information and communication relating

to the processing of your Personal Data will be easily accessible and easy to understand;

5.2 **We shall keep you informed regarding our processing of your Personal Data and provide the information regarding your rights under these Standards:** These Standards shall be publicly available on the Flex public website and also available on the Flex internal Data Privacy Portal and upon written request to the Global Data Privacy Officer. Before your Personal Data is processed, we will let you know the identity of the Flex Group company that is the Data Controller and provide you with all of the information which is required under Data Protection Laws and under these Standards;

5.3 **We shall ensure that Personal Data will only be processed for specified, explicit and legitimate purposes ("purpose limitation"):** We will ensure that the Personal Data we hold on you will be processed for specific, explicit and legitimate purposes which were determined at the time of the collection of the Personal Data and not further processed for any additional purposes which are incompatible with the initial purposes for which the Personal Data were collected;

5.4 **We shall ensure that we comply with principles of data minimisation in relation to Personal Data ("data minimisation"):** We shall ensure that our processing operations handle Personal Data which is adequate, relevant and also limited to what is necessary in relation to the purposes for which we are processing the Personal Data. We will ensure that the period for which the Personal Data are stored is limited to a strict minimum. We will not keep Personal Data for longer than is necessary for the purposes for which it is collected and processed unless it is required to be kept longer under applicable law. Personal Data will only be processed if the purposes of the processing could not be fulfilled by other means. We will limit access to Personal Data to those employees who need access to fulfil their duties. We require our vendors and suppliers to follow a similar approach to Personal Data they access in providing services to Flex.

5.5 **We ensure that Personal Data is accurate and, where necessary, kept up to date ("accuracy"):** We will ensure that Personal Data is kept up to date and is accurate. Flex provides individuals with various methods to update and correct their Personal Data including online, using self-service systems and by contacting the HR Global Business Services or the appropriate person. We will ensure that we take every reasonable step in order to ensure that Personal Data which are inaccurate are rectified or deleted without delay.

5.6 **We will ensure that Personal Data is kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the Personal Data are processed ("storage limitation"):** We will ensure that time

limits are established for the Personal Data to undergo erasure or periodic review in accordance with applicable law including Data Protection Laws.

5.7 **We use appropriate security and confidentiality safeguards to protect your Personal Data ("integrity and confidentiality"):** We use appropriate technical, organisational, administrative and physical security measures to protect your Personal Data against unauthorised or unlawful processing and against accidental loss, destruction or damage. Taking into account the state of the art, the cost of implementation of these measures and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, we impose security appropriate to the risks represented by the processing and nature of the data to be protected. In addition, in the event of a data security breach Flex will notify relevant Supervisory Authorities unless the data security breach is unlikely to result in a risk to the rights and freedoms of Data Subjects, and notify Data Subjects if the data security breach is likely to result in a high risk to the rights and freedoms of the Data Subjects.

5.8 **We shall provide you with rights of access, rectification, erasure, restriction, portability and objection to processing in accordance with the Data Protection Laws:** You shall have the right to request a copy of all Personal Data held about you. We will provide you with access to such data as required by Data Protection Laws, unless we are permitted by Data Protection Laws to refuse or only partially comply with the request (e.g. where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character). We may, where permitted by Data Protection Laws, charge a fee for this. You shall have the right to request us to correct your Personal Data if it is inaccurate, including by means of a supplementary statement if the Personal Data is incomplete. You shall also have the right, in certain circumstances, to have your Personal Data deleted, request restriction of processing of your Personal Data or object, on grounds relating to your particular situation, to the processing of Personal Data or to any direct marketing. You shall have the right, in certain circumstances, to request that we port your Personal Data to you or a third party in a structured, commonly-used and machine readable format. If you wish to exercise any of these rights you should do so by contacting the Data Privacy Liaison Officer, Global Data Privacy Officer or if you are an employee of Flex, HR Global Business Services. Further information and procedure is set out in the Global Data Subject Rights Policy which is attached at **Annex C**.

5.9 **We recognise your right to object to direct marketing:** If we use your Personal Data for direct marketing, we will only do so if we have collected your consent for such marketing or if otherwise permitted in accordance with Data Protection Laws. If you object to our use of your Personal Data for direct marketing, you should contact the Global Data Privacy Officer, HR Global

Business Services or using such other method as may be set out in the applicable marketing communication.

5.10 **We only make limited use of automated decision making:** There are requirements under the Data Protection Laws to ensure that no evaluation of, or decision about, an individual which produces legal effects or similarly significantly affects them can be based solely on automated processing of Personal Data except in limited circumstances. For example, we make use of automated decision making in certain recruitment processes to test the aptitude of a particular candidate. However, this process will usually be used in conjunction with other recruitment processes such as interviews and so are not conducted on a solely automated basis. If Flex makes significant decisions on a solely automated basis, it will, as required by Data Protection Laws, implement safeguards such as rights for individuals to obtain human intervention, express his or her point of view and contest the decision.

5.11 **We take careful precautions with respect to the processing of Special Category Data and data relating to criminal convictions and offences:** We will only process your Special Category Data and data relating to criminal convictions and offences in accordance with Data Protection Laws, including relying on at least one of the conditions set forth under GDPR which is required to process such data. This may include the use of enhanced safeguards in relation to such Special Category Data and data relating to criminal convictions and offences, where necessary.

5.12 **We take appropriate measures with respect to our use of Data Processors:** Data Processors may include a member of the Flex Group or an external vendor who processes Personal Data on behalf of a member of the Flex Group. We shall ensure that if we use any internal or external Data Processors:

(a) we will have a written contract in place with that Data Processor;

(b) the written contract will contain all the clauses that are mandatory under Article 28 of the GDPR and otherwise under Data Protection Laws;

(c) the written contract will state that the Data Processor, amongst other things:

(i) will only act on the instructions of the Data Controller; and

(ii) has a duty to notify Flex without undue delay of any personal data breaches. There may be a duty to notify Data Subjects where the personal data breach is likely to result in a high risk to their rights and freedoms. The Data Processor shall have a duty to document any Personal Data breaches comprising the facts relating to the Personal Data breach, its effects and the

remedial action taken. The documentation should be made available to the Supervisory Authority on request.

We also have in place a comprehensive audit program to ensure Data Processors comply with the above measures (see Paragraph 6.2 below).

5.13 **We shall restrict the transfer of Personal Data:** In principle, international transfers of Personal Data from the EEA to a country or territory which has inadequate Data Privacy laws are not allowed unless adequate safeguards are in place in accordance with Data Protection Laws, for example, by a member of the Flex Group (based outside the EEA) entering into these Standards or by putting in place contractual clauses (such as the EU Standard Contractual Clauses) which protect the Personal Data being transferred. We will only transfer Personal Data where such safeguards are in place in accordance with Data Protection Laws, provided that adequate protection is provided according to Articles 45, 46, 47, 48 GDPR, or that a derogation according to 49 GDPR applies (for example, where the transfer of Personal Data is to an external vendor based outside the EEA). We will ensure that all transfers of Personal Data to external vendors based outside the EEA, respect the rules relating to EU processors (as set out in Paragraph 5.12 above) in addition to the rules on transfers outside of the EEA.

6. HOW WE COMPLY WITH AND ENFORCE THE STANDARDS

6.1 **Our privacy officers:** We maintain a comprehensive network of privacy officers throughout the Flex Group who are responsible for Data Privacy within their country, region or segment, including compliance with these Standards. Each Data Privacy Liaison Officer reports into the relevant Regional Data Privacy Officer and, ultimately, to the Global Data Privacy Officer who directly reports to the Executive Board. The Flex Board comprises the Head of Legal, the Chief Financial Officer and Chief HR Officer and it reports to the Chief Executive. The Global Data Privacy Officer shall be the Data Protection Officer as defined by the Regulation and is ultimately responsible for the network of Regional Data Privacy Officers and Data Privacy Liaison Officers, the development and implementation of these Standards responding to requests from the Supervisory Authorities, and co-operating with the Supervisory Authorities and monitoring and reporting annually on compliance to the Executive Board. The Regional Data Privacy Officers and Data Privacy Liaison Officers are responsible for handling local complaints from Data Subjects, reporting Data Privacy issues to the Global Data Privacy Officer, monitoring training and compliance at a local level and assisting with responding to requests from the Supervisory Authorities, and co-operating with the Supervisory Authorities.

6.2 **Audit and compliance:** In addition, we have in place a comprehensive audit programme which includes regular internal privacy assessments covering all aspects of these Standards. The results of such privacy assessments are provided to the Global Data Privacy Officer and the Executive Board of Flex Ltd. If we identify any gaps in compliance with our Data Privacy requirements (including these Standards) work plans are put in place to rectify any gaps. Where such assessment relates to these Standards they will be provided to the competent Supervisory Authority upon request.

6.3 **Training Programme:** We take Data Privacy very seriously and evidence this by providing mandatory Data Privacy training to all employees who have permanent or regular access to Personal Data, who are involved in the collection of Personal Data or in the development of tools used to process Personal Data in carrying out their duties. In addition to this, all employees are required to comply with all Flex policies and procedures which includes these Standards and are also required to confirm acknowledgement of the Flex Code of Conduct which sets out the Flex Group's commitment to Data Privacy and confidentiality.

6.4 **Accountability:** Every Flex Group member acting as a data controller shall be responsible for and able to demonstrate compliance with the Standards where they process Personal Data described in Paragraph 4.1 of the Standards. In order to demonstrate compliance, Flex Group members will document categories of processing activities carried out in line with the requirements as set out in Art.30 GDPR This record should be maintained in writing, including in electronic form, and should be made available to the Supervisory Authority on request.

6.5 **Data Protection Impact Assessments:** In order to enhance compliance and when required, Flex Group members will carry out data protection impact assessments in consultation with the Global Data Privacy Officer for processing operations that are likely to result in a high risk to the rights and freedoms of natural persons. Where the outcome of a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by Flex Group member to mitigate the risk, the Supervisory Authority should be consulted prior to processing.

6.6 **Privacy by Design and Default:** Appropriate technical and organisational measures should be implemented by Flex Group members which are designed to implement the data protection principles under the Regulation and to facilitate compliance with the requirements set up by these Standards.

6.7 **National legislation and these Standards:** We will ensure that if applicable data protection and privacy laws provide less protection than these Standards, these Standards will apply to our processing of Personal Data. However, if applicable data protection and privacy laws provide a higher

protection, we will ensure that we will comply with the higher standard. Additionally, if a member of the Flex Group believes that a conflict with applicable data protection and privacy laws prevents it from fulfilling its duties under these Standards (including following the advice of a competent Supervisory Authority) that member entity will promptly notify the Global Data Privacy Officer or applicable Data Privacy Liaison Officer who will (in consultation with the Legal Department or the relevant Supervisory Authority, where necessary) responsibly decide what action to take.

Flex will ensure that where it has reason to believe that legislation applicable to it prevents it from fulfilling obligations under these Standards or has a substantial effect on its ability to comply with these Standards, it will promptly notify the Flex Group member with delegated data protection responsibility and the Global Data Privacy Officer unless otherwise prohibited by a law enforcement body such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

Where any legal requirement Flex is subject to in a non-EEA country is likely to have a substantial adverse effect on the protection afforded by these Standards, the problem should be reported to the Supervisory Authority. This includes any legally binding request for disclosure of the Personal Data by a law enforcement authority or state security body. The Supervisory Authority should be clearly informed about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). In these cases, the Flex member will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so. If, in the above cases, despite having used its best efforts, the Flex member is not in a position to notify the Supervisory Authority, Flex must annually provide general information on the requests it received to the Supervisory Authority (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.). In any case, the transfers of Personal Data by a Flex member of the group to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

7. RELATIONSHIP WITH THE SUPERVISORY AUTHORITIES

7.1 **Co-operation with the Supervisory Authorities:** The members of the Flex Group will co-operate with any Supervisory Authority and will provide assistance to each other in order to do so and to handle any request or complaint from a Data Subject or an investigation or inquiry. Any questions about our compliance with Data Protection Laws should be addressed to the Global Data Privacy Officer using the contact details set out at the end of these

Standards who will consult with the relevant Supervisory Authority, where applicable. Members of the Flex Group will abide by the advice of the Supervisory Authorities on any issues regarding the interpretation of these Standards in accordance with the Data Protection Laws. Each Supervisory Authority is authorised to audit any member of the Flex Group who is bound by these Standards and advise on all matters related to these Standards. Such members of the Flex Group must respect the decisions of each local Supervisory Authority to the extent consistent with Data Protection Laws and due process and without waiving any defences or rights of appeal.

8. YOUR RIGHTS UNDER THESE STANDARDS

8.1 **Our liability to you:** The policies and procedures described in these Standards are in addition to any other remedies available under applicable data protection and privacy laws or provided under our other policies and procedures. Flextronics International Gesellschaft m.b.H. has been nominated by the Flex Group as the company within the EEA with delegated responsibility for these Standards in the context of the Regulation and has sufficient assets to pay compensation for any damages resulting from a breach of these Standards. Flextronics International Gesellschaft m.b.H. will be responsible for and will take any action necessary to remedy any breach by a member of the Flex Group outside the EEA bound by these Standards. This will include any sanction imposed or other remedy available under applicable data protection and privacy laws including the requirement to pay compensation for any material or non-material damages resulting from the breach of the Standards by members of the Flex Group outside the EEA. If a member of Flex Group outside the EEA breaches these Standards, the Courts or Supervisory Authority in Austria will have jurisdiction and Flextronics International Gesellschaft m.b.H. shall be liable to you as if the breach had been caused by them in Austria instead of the Flex Group member outside the EEA. Flextronics International Gesellschaft m.b.H. shall not be liable if it is able to show that the member of the Flex Group which is alleged to be in breach is not liable for the breach giving rise to damages or that no such breach took place. The burden of proof will lie with Flextronics International Gesellschaft m.b.H. in order to demonstrate that the Flex Group member outside the EEA which is alleged to be in breach is not liable for any breach of the Standards which has resulted in the claim for damages. In each case identified above, if it is held that these Standards have been breached, it shall be the responsibility of the claimant to demonstrate that he or she has suffered damage and establish facts which show it is likely that the damage has occurred as a result of such breach.

8.2 **Your rights under these Standards:** If you believe a member of the Flex Group is in breach of these Standards, you may raise a complaint by contacting HR Global Business Services or the Global Data Privacy Officer (please see

Paragraph 10 below). Please also refer to the Global Procedure for Raising and Handling Data Privacy Complaints (a copy of which can be found on the Flex Data Privacy Portal and can be found at **Annex D** to these Standards) which sets out further detail regarding the complaints handling process. , You can enforce the rights as set out in these Standards (including those set out in Paragraphs 5, 6.4, 6.7, 7, 8.1, 8.2, 8.3 and 9.1) as a third party beneficiary, in relation to transfers of Personal Data made by a member of the Flex Group or a Data Processor appointed by a member of the Flex Group located within the EEA to a country outside the EEA. This can be done by (a) raising and bringing the issue of breach before the Supervisory Authorities where (i) you are habitually resident, or (ii) where you work, or (iii) where the breach of Data Protection Laws has taken place, or (b) bringing the issue of breach before the Courts either (i) where you are habitually resident, or (ii) in the jurisdiction of Austria, or (iii) in the jurisdiction of the member of the Flex Group that is at the origin of the transfer at your option in order to seek judicial remedies including the right to obtain compensation. The rights contained in this paragraph are in addition to and shall not prejudice any other rights or remedies that you may otherwise have at law including the right to compensation, if appropriate. Without prejudice to the provisions set out in Section 8.2, Flex will not be deemed to have breached these Standards if it has observed the appropriate standard of care in the circumstances or otherwise acted in accordance with Data Protection Law.

8.3 All data subjects who benefit from these rights as a third party beneficiary shall be provided with information as required by Articles 13 and 14 GDPR. The Standards contain the required information on their third party beneficiary rights with regard to the processing of their Personal Data and on the means to exercise those rights, in the clause relating to liability and the clauses relating to the data protection principles. These Standards are available on the Flex website, referred to in each applicable Privacy Notice and available on request from the Global Data Privacy Officer.

9. GENERAL

9.1 **Updates to these Standards:** From time to time we may amend these Standards (including to take account of modifications to the regulatory environment or the company structure). Additional members of the Flex Group may become bound by the Standards and certain members of the Flex Group may no longer be bound by these Standards. Therefore we will ensure that a fully updated list of members of the Flex Group is available from the Global Data Privacy Officer and will provide this information to Data Subjects and the Supervisory Authorities on request. The Global Data Privacy Officer will keep track of and record any updates to the Standards. In addition, all amendments to the Standards will be subject to the approval of the Global Data Privacy Officer and reported without undue delay to all Flex

Group members and to the relevant Supervisory Authorities, via the competent Supervisory Authority.

Any changes to the Standards or to the list of Flex Group members should be reported to each Supervisory Authority at least annually with a brief explanation of the reasons justifying the update. Significant changes, such as those which would possibly affect the level of protection offered by the Standards or significantly affect the Standards must be promptly communicated to the relevant Supervisory Authority and where necessary, the approval of the Supervisory Authority will be sought.

Once any amendments to the Standards are approved these will be communicated to all members of the Flex Group bound by these Standards and posted on the Flex public website and Data Privacy Portal on the Flex Group's intranet. Any revisions to the Standards shall include the date of the revision. We shall not make transfers of Personal Data covered by these Standards to a member of the Flex Group until such member is bound by these Standards and can deliver compliance.

9.2 **Effective Date:** 30 June 2015

Date of update effective from: 22 December 2020

10. CONTACT INFORMATION

Contacts: If you have any questions about these Standards, your rights under these Standards or any other privacy issues you can contact us using following email address: dataprotection@flex.com

ANNEX A – Conditions to be met by Flex prior to the processing of Personal Data

At least one of the following conditions must be met prior to the processing of Personal Data described in Paragraph 4.1 of these Standards by the Flex Group:

- The Data Subject gives his or her consent;
- The processing is necessary for the performance of a contract to which the Data Subject is a party or for taking steps at the request of the Data Subject prior to entering into a contract;
- The processing is necessary for compliance with Flex's legal obligations, other than a contractual obligation;
- The processing is necessary to protect the vital interests of the Data Subject or another natural person;
- The 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;
- The processing is necessary to pursue the legitimate interests of Flex or by a third party, 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.

At least one of the following conditions must be met prior to the processing of Personal Data described in Paragraph 4.1 of these Standards which is Special Category Data by the Flex Group:

- The Data Subject has given his or her explicit consent;
- The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- The processing relates to personal data which are manifestly made public by the data subject;

- The processing is necessary for the establishment, exercise or defence of legal claims;
- The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional;
- The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

All processing of data relating to criminal convictions and offences by the Flex Group shall be based on conditions under Data Protection Laws.

ANNEX B – Description of the Material Scope of the Standards

Transfers of Personal Data by Flex Group

1 Transfer of Employee Data

Purposes for export or import	• Recruitment including planning and implementation of recruitment strategies and staffing across the Flex Group • Recruitment and head count management • Payroll and management of employee benefits including leave administration, compensation administration, focal review, performance review and employee care services • Career and professional development and talent management • Superannuation such as pension contributions • Stock administration including management of the Employee Stock Purchase Plan, filing and reporting • Disciplinary and grievance procedures • Equal opportunities management in the US • Performance management and appraisals • Administration of personnel records and inquiry support including in relation to leave, absence, pay and benefits • Maintaining directories and facilitating records of business notices and/or communications to employees and contractors • Training administration • For fraud prevention or investigation, or other risk management purposes • On the written request of the Data Subject, where appropriate • Safety including support information for workers' compensation claims and in emergencies where the health or safety of a person is endangered • Business travel • Compliance with contractual, legal and regulatory obligations and dealing with legal claims and disputes • Other personnel matters relating to the Data Subject required or permitted by law or regulation. • Contact with next of kin • Authorisation controls and data security • Back-up and business continuity • Protecting intellectual property, confidential information and assets • Management forecasts and planning changes in group structure

Types of Data Subject	Staff including: • Current, former and prospective employees • Current, former and prospective contractors • Volunteers • Agents • Temporary and casual workers • Dependants, relatives, guardians and associates of the data subjects set out above.
Categories of Personal Data	• Personal details including names, date of birth, home address, national tax ID, social security number, drivers licence number, passport number and personal email address • Family, lifestyle and social circumstances which may include marital status, details of partner, children's details and mother's name • Education and training details including qualifications, academic records, schools, training record and professional expertise • Employment details including employment status, job role, hire date, work location, termination date, status, appraisal details and organisational details such as company employed by, office address, work phone number, individual photograph, department and supervisors, cost centre, employee type and whether full time or part time, work email address, intranet user log in, supervisor details, HR adviser details, other email addresses, job description, codes and employee ID • Financial details including benefit details, stock ownership, pay, expenses, pay cheque information and bank account information, bonus target and pensions information • Goods and services details including details of trades or products sold by Data Subjects
Type of Special Category Data or data relating to criminal convictions or offences	• Racial or ethnic origin • Religious or other beliefs of a similar nature • Trade union membership • Physical or mental health or condition • Offences (including any alleged offences)
Type of persons having access to the Personal Data	Employee Data is processed by members of the human resources department, relevant employee managers and members of the HR Global Business Services for the purposes set out above. Certain of this Employee Data may also be sent to: • Data Subjects themselves • Relatives, guardians, or other person associated with the Data Subject • Current, past or prospective employers of the Data Subject • Education, training establishment and examining bodies

	• Business associates and other professional advisers • Other Flextronics entities • Employees and agents of Flextronics • Suppliers and/or providers of goods and services • Financial organisations and advisers • Credit reference agencies • Trade, employer associations and professional bodies • Government agency and law enforcement bodies as required by law • Employment and recruitment agencies • Pension fund administrators • Certain data processors instructed by Flextronics to process the data • Potential acquirers or purchasers in relation to disposal of any Flex business or assets
Countries where Personal Data is exported from	Worldwide including Australia, Austria, Bermuda, Brazil, British Virgin Islands, Canada, Cayman Islands, Chile, China, Costa Rica, Curacao, Czech Republic, Denmark, Finland, France, Germany, Hong Kong, Hungary, India, Indonesia, Ireland, Israel, Italy, Japan, Labuan, Luxembourg, Malaysia, Mauritius, Mexico, the Netherlands, New Zealand, Philippines, Poland, Romania, Switzerland, Sweden, UK, Singapore, Spain, South Korea, Taiwan, Turkey, Ukraine and the USA.
Countries where Personal Data is exported to	Worldwide including Australia, Austria, Bermuda, Brazil, British Virgin Islands, Canada, Cayman Islands, Chile, China, Costa Rica, Curacao, Czech Republic, Denmark, Finland, France, Germany, Hong Kong, Hungary, India, Indonesia, Ireland, Israel, Italy, Japan, Labuan, Luxembourg, Malaysia, Mauritius, Mexico, the Netherlands, New Zealand, Philippines, Poland, Romania, Switzerland, Sweden, UK, Singapore, Spain, South Korea, Taiwan, Turkey, Ukraine and the USA.
Basis for onward transfer	On the basis of compliance with one or more of the conditions in Annex A to the Data Privacy Standards.

Transfer of Business Contact Information

Purposes for export or import	• Maintaining and building upon customer and supplier relationships • Business planning • To fulfil a transaction initiated by a Data Subject • To fulfil a transaction initiated by a member of the Flex Group such as the purchase of supplies or equipment • To fulfil a transaction with, or for, Flex customers • Keeping accounts related to any business or other activity carried on by Flex • Deciding whether to accept any person as a customer or supplier • Keeping records of purchases, sales or other transactions for the purpose of ensuring that the required payments and/or deliveries are made or services provided • Completion of customer satisfaction surveys • Research and development • Business development • Event management • Database management • Running competitions • Security • For fraud and theft prevention or investigation, or other risk management purposes • Compliance with contractual, legal and regulatory obligations • On the written request of the Data Subject, where appropriate
Types of Data Subject	Flex customers (including the customers of our clients), business contacts and suppliers
Categories of Personal Data	• Personal details including name, home address, employer, office address, personal and work telephone numbers and home and work email addresses. • Financial details including payments made and received and VAT/sales tax • Goods or services provided or purchased
Type of Special Category Data or data relating to criminal convictions or offences	• None
Type of persons having access to the Personal Data	Business Contact Data is used primarily by Flex employees as is necessary to fulfil their job requirements. However, Business Contact Data customer information may also be sent to: • Business associates and other professional advisers • Other employees, agents and contractors of Flextronics

	• Suppliers and/or providers of goods and services • Third parties including for the purpose of event management • Government agency, Court and law enforcement bodies as required by law • Claimants, beneficiaries, assignees and payees • Potential acquirers or purchasers in relation to disposal of any Flex business or assets
Countries where Personal Data is exported from	Worldwide including Australia, Austria, Bermuda, Brazil, British Virgin Islands, Canada, Cayman Islands, Chile, China, Costa Rica, Curacao, Czech Republic, Denmark, Finland, France, Germany, Hong Kong, Hungary, India, Indonesia, Ireland, Israel, Italy, Japan, Labuan, Luxembourg, Malaysia, Mauritius, Mexico, the Netherlands, New Zealand, Philippines, Poland, Romania, Switzerland, Sweden, UK, Singapore, Spain, South Korea, Taiwan, Turkey, Ukraine and the USA.
Countries where Personal Data is exported to	Worldwide including Austria, Brazil, Canada, China, Czech Republic, Denmark, Finland, France, Germany, Hong Kong, Hungary, India, Indonesia, Ireland, Israel, Italy, Japan, Malaysia, Mauritius, Mexico, the Netherlands, Philippines, Poland, Romania, Russia, Switzerland, Sweden, UK, Singapore, South Korea, Taiwan, Turkey, Ukraine and the USA.
Basis for onward transfer	On the basis of compliance with one or more of the conditions in Annex A to the Data Privacy Standards.

2 Transfer of other Personal Data

a. Crime prevention and prosecution

Purposes for export or import	• Crime prevention and assisting the appropriate authorities and agencies with the detection, apprehension and prosecution of offenders • The monitoring and collection of visual images for the purpose of maintaining security of the applicable Flex premises • In response to a lawful request from a court or government agency or to otherwise comply with applicable law or compulsory process
Types of Data Subject	• Flex customers and clients (including customers of our clients), business contacts and suppliers • Advisers, consultants and other professional experts • Members of the public • Flex staff including volunteers, agents, temporary and casual workers • Those inside, entering or in the immediate vicinity of the area under surveillance
Categories of Personal Data	• Personal details • Family, lifestyle and social circumstances • Education and employment details • Financial details • Goods or services provided • Sound and/or visual images
Type of Special Category Data or data relating to criminal convictions or offences	• Offences including alleged offences • Criminal proceedings, outcomes and sentences
Type of persons having access to the Personal Data	• The Data Subjects themselves • Business associates and other professional advisers • Other employees and agents of Flex • Other companies of the Flex Group • Persons making an enquiry or complaint • Government agency, Court and law enforcement bodies as required by law • Suppliers and/or providers of goods and services • Third parties providing vendor and security services
Countries where Personal Data is exported from	Worldwide including Australia, Austria, Bermuda, Brazil, British Virgin Islands, Canada, Cayman Islands, Chile, China, Costa Rica, Curacao, Czech Republic, Denmark, Finland, France, Germany, Hong Kong, Hungary, India, Indonesia, Ireland, Israel, Italy, Japan, Korea, Labuan, Luxembourg, Malaysia, Mauritius, Mexico, the Netherlands, New Zealand, Philippines, Poland, Romania, Switzerland, Sweden, UK, Singapore,

	Spain, South Korea, Taiwan, Turkey, Ukraine and the USA.
Countries where Personal Data is exported to	Worldwide including Australia, Austria, Bermuda, Brazil, British Virgin Islands, Canada, Cayman Islands, Chile, China, Costa Rica, Curacao, Czech Republic, Denmark, Finland, France, Germany, Hong Kong, Hungary, India, Indonesia, Ireland, Israel, Italy, Japan, Labuan, Luxembourg, Malaysia, Mauritius, Mexico, the Netherlands, Philippines, Poland, Romania, Switzerland, Sweden, UK, Singapore, Spain, South Korea, Taiwan, Turkey, Ukraine and the USA.
Basis for onward transfer	On the basis of compliance with one or more of the conditions in Annex A to the Data Privacy Standards.

b. Managing Shareholdings

Purposes for export or import	• Deciding whether to accept any person as a shareholder • Keeping records and administering stock purchases or other relevant transactions • For fraud prevention or investigation, or other risk management purposes • To prospective purchasers and for protecting Flex legal rights or assets to facilitate the acquisition or disposition of Flex businesses • In response to a lawful request from a Governmental agency, Court and law enforcement body and to otherwise comply with applicable law or compulsory process
Types of Data Subject	• Shareholders and contacts of shareholders
Categories of Personal Data	• Personal details including contact information • Financial details
Type of Special Category Data or data relating to criminal convictions or offences	None
Type of persons having access to the Personal Data	Personal data is used primarily by Flex employees as is necessary to fulfil their job requirements and administer shareholder benefits. However personal data may also be sent to: • The Data Subjects themselves • Business associates and other professional advisers • Other employees and agents of Flex • Other companies of the Flex Group • Potential acquirers or purchasers in relation to disposals of any Flex business or assets • Government agency, Court or law enforcement body as required by law • Ombudsmen and regulatory authorities
Countries where Personal Data is exported from	Worldwide including Australia, Austria, Bermuda, Brazil, Canada, Cayman Islands, Chile, China, Costa Rica, Curacao, Czech Republic, Denmark, Finland, France, Germany, Hong Kong, Hungary, India, Indonesia, Ireland, Israel, Italy, Japan, Labuan, Luxembourg, Malaysia, Mauritius, Mexico, the Netherlands, New Zealand, Philippines, Poland, Romania, Switzerland, Sweden, UK, Singapore, Spain, South Korea, Taiwan, Turkey and Ukraine and the USA.
Countries where Personal Data is exported to	Worldwide including Australia, Austria, Bermuda, Brazil, British Virgin Islands, Canada, Cayman Islands, Chile, China, Costa Rica, Curacao, Czech Republic, Denmark, Finland, France, Germany, Hong Kong, Hungary, India, Indonesia, Ireland, Israel, Italy, Japan,

	Labuan, Luxembourg, Malaysia, Mauritius, Mexico, the Netherlands, New Zealand, Philippines, Poland, Romania, Switzerland, Sweden, UK, Singapore, Spain, South Korea, Taiwan, Turkey and Ukraine and the USA.
Basis for onward transfer	On the basis of compliance with one or more of the conditions in Annex A to the Data Privacy Standards.

ANNEX C - GLOBAL DATA SUBJECT RIGHTS POLICY

1 Introduction

1.1 Purpose of this Global Data Subject Rights Policy

(a) Flextronics (Flex) is committed to privacy and respecting the rights of those whose personal data Flex collect and use. Supporting privacy requires all of us to have an awareness of the rights which individuals have over the data belonging to them which we collect or hold.

(b) Every individual whose personal data we hold and use has rights in respect of that data. This includes employees, business contacts, and website users. This policy is to enable us to respect those rights in accordance with our Data Privacy Standards.

(c) The individual rights contained in this Policy reflect those rights outlined in the Data Privacy Standards and at Section 7 of the Flex Global Privacy Policy and Rules.

(d) Flex support the entitlement of individuals to exercise their rights to protect and verify the correct use of their personal data. Flex will respond in a quick and helpful manner if an individual asks us a question about the personal data Flex hold about them. Flex will facilitate individuals to exercise these rights and, where practicable, provide electronic means for these rights to be exercised.

(e) Individuals may contact Flex verbally or in writing to request that Flex take some action in connection with their personal data. Requests should be referred to the local Data Privacy Liaison Officer for your jurisdiction in the first instance, or to the Global Data Privacy Officer, who is the Data Protection Officer for the purposes of the EU General Data Protection Regulation ("GDPR") and can be contacted on: dataprotection@flex.com or +43 1 602 4100 1737.

(f) This policy explains how Flex identify and respond to requests from individuals concerning their data.

(g) In general, Flex must respond to queries within one month from the receipt of the request, so it is important that requests are identified and handed to the correct people within Flex as soon as possible.

(h) Our key objectives when handling requests from individuals are to:

(i) **identify** the nature of the request at the earliest opportunity;

(ii) **respond** to the individual making the request in a timely manner;

(iii) **work with** the individual making the request to understand their request, their concerns and how we can assist; and

(iv) **maintain clear records** regarding each request we receive and our response.

1.2 What rights do individuals have?

(a) Individuals have the right to make the following types of request regarding the personal data Flex holds about them:

(i) **Right of access (subject access requests)** – the right to request a copy of the personal data that Flex have concerning the individual and supporting information explaining how the personal data is used.

(ii) **Right of rectification** – the right to request that we rectify inaccurate personal data concerning the individual.

(iii) **Right of erasure** (**right to be forgotten**) – the right, in some situations, to request that Flex erase all personal data concerning the individual.

(iv) **Right to restrict processing** – the right, in some situations, to request that Flex do not use the individual's personal data they have provided (e.g. if they believe it to be inaccurate).

(v) **Right to data portability** – the right, in some situations, to request that Flex port the individual's data to that individual or their new provider in machine readable format.

(vi) **Right to object** – the right to object to certain processing of their personal data (unless Flex have overriding compelling grounds to continue the processing) and the right to object to direct marketing/profiling.

(vii) **Rights relating to automated decision making** – the right not to be subject to automated decision making that significantly affects an individual (e.g. certain profiling).

(b) Flex will respond to requests listed in 1.2(a) above in accordance with Annex C 1.1(g). However, in certain circumstances that period may be extended by a further two months, taking into account the complexity of the request(s) and the number of requests made. If applicable, the GDPO, in consultation with the Legal Team, will take this decision and notify the Data Subject within one month of the receipt of the request, together with the reasons for the delay. Where the Data Subject has made the request by electronic form means, the information shall be

provided by electronic means where possible, unless otherwise requested by the Data Subject.

2 Roles and Responsibilities

Role	Responsibility
Data Subject	An individual who has the right to raise an individual rights request / data subject rights request.
Data Privacy Liaison Officer (DPLO)	Responsible for escalating individual rights requests for their jurisdiction and for the tasks set out at Section 6 of the Flex Global Privacy Policy and Rules. Report to their relevant Regional Data Privacy Officer.
Regional Data Privacy Officer (RDPO)	Responsible for the tasks set out at Section 6 to the Flex Global Privacy Policy and Rules and for compliance with the Data Privacy Standards. Report to the Global Data Privacy Officer.
Global Data Privacy Officer (GDPO or DPO)	The Data Protection Officer for the purposes of the EU General Data Protection Regulation ("GDPR"). Responsible for tasks as set out in Section 6 of the Flex Global Privacy Policy and Rules and responsible for the network of Regional Data Privacy Officers, Data Privacy Liaison Officers, the development and implementation of the Data Privacy Standards, responding to requests from the Supervisory Authorities, and co-operating with the Supervisory Authorities. May delegate tasks within this Policy to the RDPO.

3 Identifying individual rights requests

(a) Identifying requests from individuals regarding their personal data is crucial and requires **the support of everyone within Flex.**

(b) **It is essential that we identify and notify the relevant people within Flex once we receive a request from an individual**.

(c) Flex are required to respond to, and address, requests within **one month** of receiving them. Flex must therefore act quickly and effectively.

3.1 Identifying the individual rights request

(a) Requests relating to personal data may not always be completely obvious or clear. Requests **may refer to data protection law**, e.g. the EU General Data Protection Regulation or "GDPR" but requests **do not need to refer to any law** to be valid.

(b) **Listen and look for key words and phrases** to identify whether a particular communication is a request concerning personal data. The following keywords and phrases are a non-exhaustive list of indicators:

(i) Can you please **give me** / **provide me with** / **send me** all the personal information Flex holds about me.

(ii) **Are you** using my data / **why** are you using my data / **how** are you using my data / **who** are you sharing my data with?

(iii) You have the **wrong** [address, date of birth, surname, sex etc.] for me, please **change** it to…

(iv) **Delete** / **remove** / **purge** all information you have about me.

(v) **Stop** using my information, it is **against the law** for you to use it in this way / it is **inaccurate** / you do not **need** to use it any more / I **don't want** you to use it for…."

(vi) "**Give** me all my data to…. "

(c) Flex, through its Global Business Services (**GBS**) maintains a dedicated email address for subjects to submit individual rights requests. The address is dataprivacy@flextronics.com. However rights requests can be made by any means, e.g. **in person**, on the **phone**, by **email**, **letter or fax**. It is also possible to receive more than one form of rights request in the same communication.

(d) **If you identify a request as one which does, or which may, concern personal data, immediately inform the Data Privacy Liaison Officer (DPLO).**

(e) If you cannot be certain that the request is legitimate or that the person making the request is who they say they are, then take common sense steps to check. For example, call a number provided by the individual to check they have made the request or ask them to send an email from a recognised account. If you are still not certain about the identity of the person making the request, liaise with the Global Data Privacy Officer (GDPO) to determine what further steps should be taken.

4 Reporting and responding to requests from individuals

(a) When you receive something that looks like it is, or may be, a request concerning personal data, please **notify the DPLO immediately**. Speak to your line manager or the Legal team if you do not know the identify of the DPLO or if they are unavailable.

(b) The GDPO will work with the DPLO to request all information from the reporting individual as may be necessary to identify the nature of the request, for example requesting a copy of the individual's passport, and/or a recent utility bill.

(c) The GDPO will determine whether or not the request is a valid request regarding personal data and ensure that Flex has acknowledged receipt of the request to the relevant individual.

(d) It is also possible that individual rights requests can also be made via a third party. Often this will be a solicitor acting on behalf of the individual. In these cases, Flex will validate that the third party has been authorised to make a request on behalf of the individual. The third party will need to provide evidence of this authorisation. The evidence can be in a written format to grant the third party to make such request or it could also be a general power of attorney.

(e) The GDPO will identify the category of the request and respond in accordance with the relevant process set out below and Flex obligations under data protection law. The GDPO will work with support from the DPLO, RDPO, your line manager, IT and the Legal team when responding to requests.

(f) The GDPO shall periodically review the total number of requests that are received and whether such requests have been dealt with in accordance with this policy and, where appropriate, shall review any underlying issues giving rise to requests.

(g) Once a request from an individual has been identified, the GDPO shall follow the relevant process outlined below.

4.1 Right of Access (subject access request)

(a) You will work with the GDPO and the IT team to progress an access request by arranging a search of all our relevant systems for the appropriate personal data (including local storage such as shared and personal drives), email servers, back-up locations and third party applications on which personal data is stored on our behalf, and under our instruction, of (e.g. HR systems, CRM platforms, accounting programs etc.). Have the individual complete an individual rights request form, if possible. Copies of forms will be available on the Portal.

(b) The **search process shall be started as soon as possible** as it can be a detailed and time consuming exercise.

(c) **All relevant teams/departments** should be contacted to ensure that all relevant file, folders (whether electronic or paper) and third party applications are searched.

(d) Where a general request is made for "all information held by Flex", the search criteria should be as broad as possible in the first instance to identify all possible documents relating to the individual. Search criteria such as the individual's name, address, initials, alias etc. should be used to assist. The individual's personal data may appear in letters, memos, e-mails, file notes, electronic address books etc. as well as in our customer or HR database and in customer profiles.

(e) Upon completion of the search you will work with the GDPO (and the Legal team, if necessary) to prepare and respond to the individual, providing copies of the relevant personal data and associated information that the individual is legally entitled to receive.

(f) All responses must be signed off by the GDPO, and contain the following information:

(i) the purposes of the processing;

(ii) the categories of personal data concerned;

(iii) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in non-EEA countries or international organisations (and information on the appropriate safeguards used for international transfers, if relevant);

(iv) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(v) the existence of the right to request from Flex rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(vi) the right to lodge a complaint with a Supervisory Authority;

(vii) where the personal data are not collected from the data subject, any available information as to their source (such as from third party partners); and

(viii) the existence of any automated decision-making, including profiling, applied to any of their data, information about the

logic involved as well as the significance and the envisaged consequences of such processing for the data subject**.** **Disclosure of information about profiling is only necessary where the profiling produces a legal effect or otherwise will significant affect the relevant individual** e.g. determines whether an individual gets a job or promotion; or determines the price at which any product or service is offered to them or targets vulnerable groups of people.

(g) If the subject access request is made in electronic form (e.g. by email), the information should be provided in a commonly used electronic form, for example, in PDF, Word or Excel (unless the data subject requests otherwise).

(h) **Exemptions**:

(i) Flex should not provide data to the individual if to do so adversely affects the rights of others (data concerning the individual that does not affect others must still be provided, such as where the data discloses information about third parties which could adversely affect them).

(ii) If Flex hold a large quantity of data concerning the individual, Flex can ask the individual to specify the information or use of data that their request relates to – but Flex must still respond to the request once we identify the information.

(iii) Flex should not provide information which is subject to legal privilege.

(i) If the GDPO believes an exemption may apply, the GDPO will notify the Legal team and a decision must be made jointly between the GDPO and Legal team.

(j) **Timing**

(i) Flex must provide this information to an individual **without undue delay** and **within one month** of receiving the request, at the latest.

(ii) If the GDPO, working with the Legal team where necessary, determines that an exemption applies, the GDPO shall notify the individual making the request **without undue delay** and **within once month** with an explanation of the reasons why Flex will not comply with their request.

(k) **Record Keeping**

The HR Global Business Services team will maintain complete records of the process and response for each request.

4.2 Right of rectification

(a) You will work with the GDPO and IT team to **locate** the data the individual claims to be incorrect and, if the circumstances are as the individual described, correct the data on all our files and systems where it is stored.

(b) If the individual asks for incomplete data to be completed you will work with the GDPO and IT team to complete the data. This includes enabling the individual to give a supplementary statement to complete the data.

(c) You will work with the GDPO to inform the individual that the information has been corrected / completed as soon as possible.

(d) **Time period**

(i) Flex must rectify / complete the information in question **without undue delay** and **within one month** of receiving the request, at the latest.

(e) **Record Keeping**

(i) The HR Global Business Services team will maintain complete records of the process and response for each request.

4.3 Right of Erasure (the right to be forgotten)

(a) This right is only available in certain circumstances (set out below). The GDPO will first assess whether the individual actually has this right before liaising with the HR Information Systems team to carry out the erasure.

(b) **This right <u>only</u> applies when**:

(i) the data is no longer necessary for the purpose for which they were collected or processed;

(ii) the individual withdraws consent to processing (and there is no other justification for processing);

(iii) the individual objects to Flex's use of their data and Flex cannot demonstrate that there are overriding legitimate grounds for processing;

(iv) Flex have used their data unlawfully; or

(v) the data must be deleted to comply with law.

(c) If the GDPO concludes that this right applies, this conclusion will be referred to the Legal team for review. If the Legal team and the GDPO agree that the right applies, the IT team will assist in deleting the relevant data from our systems (and any third party systems on which the individual's data is stored (e.g.IT hosting providers, database providers, etc.)

(d) If the data has been made public by Flex, it is also necessary to inform others who may be using that data (e.g. partners, linked social media sites, etc.) that the individual has requested their data is to be deleted. Flex will take reasonable steps to do this (taking into account the available technology and cost of implementation). The GDPO, working with the Legal team where necessary, will decide what these reasonable steps are.

(e) **Exemptions**

(i) Flex are not required to comply with a request to erase data if processing the data is necessary:

(A) to exercise freedom of expression and information;

(B) to comply with law;

(C) for public health reasons;

(D) for archiving purposes in the public interest

(E) scientific or historical research purposes or statistical purposes; or

(F) if required in connection with legal claims;

(ii) Flex are also not required to comply if the request is manifestly unfounded or excessive (in particular where the same individual has made the same request on multiple occasions).

(iii) If the GDPO believes an exemption may apply, the GDPO will notify the Legal team and a decision will be made jointly between the GDPO and the Legal team.

(f) **Time period**

(i) Flex must erase this information **without undue delay** and **within one month** of receiving the request, at the latest.

(ii) If the GDPO, working with the Legal team where necessary, determine that an exemption applies, the GDPO shall notify the individual making the request **without undue delay** and **within once month** with an explanation of the reasons why Flex will not comply with their request.

(g) **Record Keeping**

(i) The HR Global Business Services team will maintain complete records of the process and response for each request.

4.4 Right to restrict processing

(a) An individual may request that Flex restrict the processing of their personal data in certain circumstances.

(b) This right only applies when:

(i) the individual disputes the accuracy of the data Flex hold;

(ii) the individual objects to the processing and Flex are determining whether there are legitimate grounds on which to continue processing their personal data;

(iii) the processing is unlawful but the individual objects to erasure and requests restriction instead;

(iv) Flex have no further need for the data but the individual requires it in connection with a legal claim.

(c) In each of the scenarios outlined above, Flex can be required to restrict use of the data until the situation is resolved; however, Flex may continue to store the data. This right is intended as a temporary measure only.

(d) When data is restricted, Flex may only store the data. Otherwise it must not be used unless:

(i) the individual consents;

(ii) its use is necessary in connection with a legal claim; or

(iii) it is required for public interest reasons.

(e) The GDPO shall assess whether the right applies, and if it does, shall work with the IT team to restrict the processing of the relevant data.

(f) Where the data in question is ordinarily processed automatically, the GDPO shall instruct the IT team to put measures in place to isolate or block the data in question.

(g) The GDPO shall work with the Business Unit that process the personal data to ensure that all relevant staff are aware of the restrictions in place.

(h) The GDPO, working with the Legal team where necessary, may determine that the restriction no longer applies as the requirements above can no longer be met. Prior to unrestricting the processing of the data, the GDPO must first inform the relevant individual.

(i) **Time period**

(i) Flex must respond to a request to restrict processing **without undue delay** and in any event **within one month** of receiving the request.

(j) **Record Keeping**

(i) The HR Global Business Services team will maintain complete records of the process and response for each request.

4.5 Right to data portability

(a) An individual may request that we transfer certain data held about them to the individual or to another entity.

(b) This right only applies:

(i) to data which the individual has provided to Flex (and therefore does not apply to data which Flex have created about the individual). However, information about how an individual uses a product or service or device will be considered as "provided by" the individual;

(ii) where the processing of the relevant data was based on the individual's consent or a contract with the individual; and

(iii) the processing is carried out by automated means.

(c) If the right applies, Flex must provide the relevant data to the individual in a structured, commonly used and machine readable form. This means an excel spreadsheet, word document or other common text file.

(d) The purpose of this right is to enable the information to be used by a third party provider, so this goes further than the right to access.

(e) If the individual requests that their data is transferred directly to another entity, Flex must do this where it is technically feasible.

(f) **Exemption**

(i) Flex do not have to port the data if to do so would adversely affect the rights of other individuals. This would apply where the information to be "ported" includes information about third party individuals if that information will be used for different purposes;

(ii) Flex do not have to port the data if it would result in our intellectual property rights being infringed or our trade secrets being revealed. However, if the information can be released without interfering with these rights, it should be released that way.

(g) If the GDPO believes an exemption may apply, the GDPO will notify the Legal team and a decision will be made jointly between the GDPO and the Legal team.

(h) **Time period**

(i) Flex must port this information to an individual or another **company without undue delay** and **within one month** of receiving the request, at the latest.

(ii) If the DPO, working with the Legal team where necessary, determine that an exemption applies, the GDPO shall notify the individual making the request **without undue delay** and **within once month** with an explanation of the reasons why Flex will not comply with their request.

(i) **Record Keeping**

(i) The HR Global Business Services team will maintain complete records of the process and response for each request.

4.6 Right to object (including to direct marketing)

(a) An individual may inform us that he/she objects to our processing their personal data.

(b) This right only applies where Flex are processing the individual's personal data on the basis of its or a third party's legitimate interests (rather than having obtained consent for such processing or such processing being required to provide requested products or services to the individual) and Flex cannot demonstrate that such legitimate interests override the individual's own rights, or that the processing is necessary for Flex's legal rights.

(c) The GDPO, together with the Legal team (if required), shall assess whether Flex (or a relevant third party) have any continuing legitimate interests which overrides the rights and freedoms of the individual, taking into consideration any specific circumstances, which Flex are aware of, relating to that individual.

(d) If the GDPO and the Legal team determine that Flex (or the third party) has no continuing overriding legitimate interests, Flex shall cease to process that individual's personal data. The personal data shall be deleted from the Flex systems (and third party systems).

(e) Separately, an individual may request that Flex cease to use their personal data for direct marketing, including for any profiling that Flex undertake in connection with such marketing.

(f) Upon receipt of a request to cease using personal data for direct marketing, the GDPO shall inform the relevant operational and marketing teams who shall cease using the individual's personal data for marketing as soon as possible and shall cease sending any marketing to that individual. All profiling of that individual carried out in connection with the marketing must also cease.

(g) **Time period**

(i) We must respond to such requests and, where applicable, cease the relevant processing **without undue delay** and **within one month** of receipt of the request.

(h) **Record Keeping**

(i) The HR Global Business Services team will maintain complete records of the process and response for each request.

4.7 Rights where automated decision making takes place

(a) This right applies where Flex use solely automated means to make a decision that significantly affects an individual. This might include decisions on employment or promotion based solely on aptitude tests or introduction of psychometric testing. It might also apply where we generate targeted messages to users which adjust price for the individual or specifically exploit vulnerable groups.

(b) An individual may inform Flex that he or she objects to a significant decision being made about him or her by us based solely on automated processing.

(c) Where such a request is received the GDPO, together with the Legal team, shall assess whether an exemption applies.

(d) Exemptions

(i) The automated decision is required to enter into, or perform, a contract with the individual.

(ii) The automated decision is authorised by local law of an EU member state.

(iii) Flex have the explicit consent of the individual to make such a decision.

(e) If such an exemption does not apply, Flex shall not make such a decision based solely on automated means. Instead, any such decision shall be re-considered by an appropriate member of the relevant team/Business Unit.

(f) Where an exemption does apply, Flex may continue with such decision but shall:

(i) ensure the information used to make such information is accurate and up-to-date;

(ii) consider whether it is reasonable to make the decision without using automated means;

(iii) allow human intervention into the decision-making process where requested by the individual; and

(iv) consider any objections to the decision raised by the individual as soon as reasonably possible and, ideally, within the same one month period in which the initial response is required.

(g) **Time period**

We must respond to such requests and, where applicable, cease the relevant processing **without undue delay** and **within one month** of receipt of the request.

(h) **Record Keeping**

(i) The HR Global Business Services team will maintain complete records of the process and response for each request.

ANNEX D - GLOBAL PROCEDURE OF RAISING AND HANDLING DATA PRIVACY COMPLAINTS

Introduction, Purpose & Definitions

1.1 Introduction

(a) Flextronics (Flex) is committed to data privacy and the fair processing of Personal Data, including enabling individuals to exercise the rights in respect of their Personal Data to which they are entitled under our Data Privacy Standards and applicable local data privacy laws.

(b) Many privacy regimes (including privacy laws of the European Economic Area ("EEA")), which comprises the Member States of the European Union as well as Iceland, Liechtenstein and Norway) often grant individuals certain rights in respect of the collection and processing of their Personal Data by organisations. Flex commits to respecting and enabling individuals to exercise these rights, as set out in our Data Privacy Standards and the Global Data Subject Rights Policy.

(c) A Data Subject has a right to raise a Data Privacy Complaint relating to any processing of their Personal Data by Flex or a Flex entity.

1.2 Purpose of the Policy

(a) The purpose of this policy is to set out the procedure which is to be followed by:

(i) Individuals (Data Subjects) who submit a Data Privacy Complaint; and

(ii) Flex when a Data Privacy Complaint is received.

1.3 Definitions

(a) **Data Privacy Complaints:** A complaint or concern about data privacy matters made against a person or entity, including a complaint that Flex or a specific Flex entity is not complying with the Data Privacy Standards, any Flex policies relating to data privacy or applicable data privacy laws.

(b) **Business Contact:** A business contact at any clients, underlying investors, shareholders, suppliers, partners or vendors.

(c) **Data Subject:** All individuals whose Personal Data is processed by one or more Flex entities, including current and former employees, Business

Contacts and any other data subjects. A Data Subject has a right to raise a Data Privacy Complaint pertaining to any processing of their Personal Data by Flex or a Flex entity.

(d) **Personal Data:** information relating to an identified or identifiable individual 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. Examples include, but are not limited to:

(i) name, address, Tax Identification Number, Social Security Number, National Identity number, date of birth, personal account numbers, credit/debit card numbers, online banking user names (whether or not used together with passwords);

(ii) data revealing racial or ethnic origin, political opinions, religious beliefs, union membership status, physical or mental health or condition, sexual life and criminal history.

2 Roles and Responsibilities

Role	Responsibility
Data Subject	An individual who has the right to raise a Data Privacy Complaint.
Data Privacy Liaison Officer (DPLO)	Responsible for escalating all Data Privacy Complaints to the GDPO and the tasks set out at Section 6 to the Flex Global Privacy Policy and Rules. Report to their relevant Regional Data Privacy Officer.
Regional Data Privacy Officer (RDPO)	Responsible for the tasks set out at Section 6 to the Flex Global Privacy Policy and Rules and for compliance with the Data Privacy Standards. Report to the Global Data Privacy Officer.
Global Data Privacy Officer (GDPO or DPO)	The Data Protection Officer for the purposes of the EU General Data Protection Regulation ("GDPR"). Responsible for tasks as set out in Section 6 of the Flex Global Privacy Policy and Rules and responsible for the network of Regional Data Privacy Officers, Data Privacy Liaison Officers, the development and implementation of the Data Privacy Standards, responding to requests from the Supervisory Authorities, and co-operating with the Supervisory Authorities. May delegate tasks within this Policy to the RDPO.

3 Receipt of a Data Privacy Complaint

3.1 A Data Subject may submit a Data Privacy Complaint by contacting HR Global Business Services (GBS) and the Global Data Privacy Officer through the following email address: data protection@flex.com.

3.2 Flex, through its Global Business Services (GBS) maintains the above dedicated email address for subjects to submit Data Privacy Complaints. However Data Privacy Complaints can be made by any means, e.g. in person, on the phone, by email, letter or fax. Flex will make available template complaint forms to assist Data Subjects and copies of forms will be available on the Flex Website and Data Privacy Portal.

3.3 Notwithstanding the above, if a Data Subject submits a Data Privacy Complaint through any other written or verbal means, a member of staff who receives such a Data Privacy Complaint will immediately forward that Data Privacy Complaint to the Global Data Privacy Officer using the above email address.

4 Complaint Handling Timelines

The following timeframe will apply to data privacy complaints handled under this Procedure.

Acknowledge receipt of complaint	Within seven (7) days	Flex to acknowledge receipt of each Data Privacy Complaint by email within seven (7) days of receipt.
Request further Information	Within fourteen (14) days	If the Data Subject fails to provide sufficient information, the Global Data Privacy Officer may request, within fourteen (14) days of receiving the Data Privacy Complaint, more information about the complaint.
Make a decision	Without undue delay and in any event within one (1) month	The Global Data Privacy Officer will consider the Data Privacy Complaint and any supplementary information provided. The GDPO will make a decision without undue delay and in any event within one (1) month of receipt of the complaint. If there are any delays in the anticipated timescales for the response, the GDPO will keep the Data Subject informed at all stages throughout the process.

If the complaint is complex or there are numerous complaints	Within three (3) months	Taking into account the complexity and number of Data Privacy Complaints, the one month period for making a decision may be extended by a maximum of two further months. The decision will be made without undue delay and in any event within three (3) months from date of receipt of the complaint. The Data Subject should be informed of this by the GDPO in writing within one (1) month of receipt of the complaint.

4.1 The Global Data Privacy Officer's decision will be in writing.

4.2 The decision of the Global Data Privacy Officer will contain at least the following information:

(a) a description of the Data Privacy Complaint,

(b) a description of the respondent's response(s), if any, to the Data Privacy Complaint;

(c) and a statement of the Global Data Privacy Officer's findings and conclusions.

4.3 The Global Data Privacy Officer shall arrange for a copy of the decision to be mailed to the complainant within three business days of the date of the decision.

5 Consequences of the Decision

5.1 In the event that the Data Privacy Complaint is upheld, the Global Data Privacy Officer will make arrangements for appropriate steps to be taken in consultation with the Legal Team, including any compensation to be paid to the Data Subject for material or non-material damages, where appropriate.

5.2 In the event that the Data Privacy Complaint is rejected, or the Data Privacy Complaint is upheld but the Data Subject is not satisfied with the proposed response, the Data Subject will have a right to any of the following:

(a) raise the issue before the Supervisory Authorities where:

(i) the Data Subject is habitually resident, or

(ii) where they work, or

(iii) where the breach has taken place.

(b) raise the issue before the Courts where:

(i) the Data Subject is habitually resident, or

(ii) in the jurisdiction of Austria, or

(iii) in the jurisdiction of the member of the Flex Group that is at the origin of the transfer which is the subject of the Data Privacy Complaint.

6 Complaint Escalation

6.1 When it is determined that a Data Privacy Complaint could pose a risk to Flex or is otherwise significant, it may require escalation to the Chief Compliance Officer.

7 Record Keeping

7.1 All relevant documentation in relation to this procedure must be recorded and maintained by GBS.

7.2 Data Privacy Complaint records shall include a copy of the Data Privacy Complaint and all communications and responses should be retained.

8 Compliance and Audit

8.1 This procedure is subject to periodic risk-based monitoring by the Flex data privacy network and compliance team to ensure that it is effective and remains fit for purpose. Additionally, it may also be subject to an independent review by the Flex internal audit team.

9 Effect of other Applicable Laws

9.1 If the Data Privacy Complaint concerns the behaviour or conduct of another specifically-identified individual, the Data Privacy Complaint will be handled in accordance with any rights that such individual may have under applicable local law, including (if applicable) the right of that individual to submit a response to the Data Privacy Complaint.

10 Training

10.1 Regional Data Privacy Officers and Data Privacy Liaison Officers will provide training to relevant staff on the procedures set out in this document. Regional Data Privacy Officers and Data Privacy Liaison Officers may train the Business Units or GBS department on identifying common issues arising in relation to the handling of Data Privacy Complaints.

11 Administrative Information

(a) Any questions relating to the interpretation and application of this policy should be addressed to the Global Data Privacy Officer at dataprotection@flex.com

(b) In the event of any inconsistency between the guidance provided in this policy and the Data Privacy Standards or any other standard, policy or procedure, please consult with the Global Data Privacy Officer.