LinkedIn Data Processing Agreement

December 12, 2022

Table of Contents

- ***LinkedIn Data Processing Agreement (DPA)***
- ***Schedule A****: Description of the Transfer*
- ***Schedule B****: CCPA Addendum*
- ***Schedule C****: Glint Specific Terms and Amendments*
- ***Schedule D:*** *Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data*

This Data Processing Agreement (the "DPA"), entered into by the LinkedIn customer identified on the applicable LinkedIn ordering document for LinkedIn services ("Customer") and the LinkedIn company identified on the ordering document (along with its affiliates, "LinkedIn"), governs the processing of Personal Data that Customer uploads or otherwise provides LinkedIn in connection with the services, the processing of Personal Data by LinkedIn on behalf of Customer in connection with the services, and the processing of any Personal Data that LinkedIn uploads or otherwise provides to Customer in connection with the services. Terms specific to LinkedIn's Glint services are provided as Schedule C to this DPA.

This DPA is incorporated into the relevant LinkedIn services agreement attached to or incorporated by reference into the ordering document previously executed by Customer, referred to generically in this DPA as the "LinkedIn Contract". Collectively, the DPA (including the SCCs, as defined herein), the LinkedIn Contract, and the applicable ordering documents are referred to in this DPA as the "Agreement". In the event of any conflict or inconsistency between any of the terms of the Agreement, the provisions of the following documents (in order of precedence) shall prevail: (a) the SCCs; (b) the applicable ordering document to the LinkedIn Contract; (c) this DPA; (d) the LinkedIn Contract. Except as specifically amended in this DPA, the LinkedIn Contract and applicable ordering document remain unchanged and in full force and effect.

1. DEFINITIONS

"CCPA" means the California Consumer Privacy Act of 2018 together, as amended by the California Privacy Rights Act of 2020, with any subordinate legislation or regulations.

"Customer Personal Data" means Personal Data that Customer uploads or otherwise provides LinkedIn in connection with its use of LinkedIn's services.

"Data Protection Requirements" means the General Data Protection Regulation, and any applicable laws, regulations, and other legal requirements relating to (a) privacy, data security, and protection of Personal Data; and (b) the Processing of any Personal Data. Data Protection Requirements may include, but are not limited to, UK GDPR, the Swiss Federal Act on Data Protection 2020, Lei Geral de Proteção de Dados (Brazil's General Data Protection Law), the CCPA, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act.

"EU Personal Data" means Personal Data the sharing of which pursuant to this Agreement is regulated by the General Data Protection Regulation.

“General Data Protection Regulation” or "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council together with any subordinate legislation or regulation implementing the General Data Protection Regulation.

“Personal Data” means information about an individual that (a) can be used to identify, contact or locate a specific individual; (b) can be combined with other information that can be used to identify, contact or locate a specific individual; or (c) is defined as “personal data” or “personal information” by applicable laws or regulations relating to the collection, use, storage or disclosure of information about an identifiable individual.

“Personal Data Breach” means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.

“Process” and its cognates mean 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“SCCs” means the European Commission Standard Contractual Clauses entered into between the parties under the Agreement.

“Subprocessor” means any entity which provides processing services to LinkedIn in furtherance of LinkedIn’s processing of Customer Personal Data.

“Supervisory Authority” means an independent public authority which is (i) established by a European Union member state pursuant to Article 51 of the General Data Protection Regulation; or (ii) the public authority governing data protection, which has supervisory authority and jurisdiction over Customer

"UK GDPR" means the UK General Data Protection Regulation, amended by the Data Protection Act 2018.

"UK Personal Data" means Personal Data the sharing of which pursuant to this Agreement is regulated by the UK GDPR.

2. NATURE OF DATA PROCESSING

Each party agrees to Process Personal Data received under the Agreement only for the purposes set forth in the Agreement. For the avoidance of doubt, the categories of Personal Data Processed and the categories of data subjects subject to this DPA are described in Schedule A to this DPA.

3. COMPLIANCE WITH LAWS

The parties shall each comply with their respective obligations under all applicable Data Protection Requirements.

4. CUSTOMER OBLIGATIONS

4.1 Customer agrees to: (i) determine the purposes and general means of LinkedIn’s Processing of Customer Personal Data in accordance with the Agreement; and (ii) comply with its protection, security and other obligations with respect to Customer Personal Data prescribed by Data Protection Requirements for data controllers.

4.2 Customer agrees to, at LinkedIn's request, designate to LinkedIn a single point of contact (the "**Master Admin**") responsible for (i) receiving and responding to data subject requests LinkedIn receives from Customer data subjects relating to Customer Personal Data; and (ii) notifying LinkedIn of Customer's intended response to a data subject request relating to the access to or the rectification, erasure, restriction, portability, blocking or deletion of Customer Personal Data that LinkedIn processes for Customer, and authorizing LinkedIn to fulfill such responses on behalf of Customer.

5. LINKEDIN OBLIGATIONS

5.1 Processing Requirements. LinkedIn will:

a. Process Customer Personal Data (i) only for the purpose of providing, supporting and improving LinkedIn's services (including to provide insights and other reporting), using appropriate technical and organizational security measures; and (ii) in compliance with the instructions received from Customer. LinkedIn will not use or Process the Customer Personal Data for any other purpose. LinkedIn will promptly inform Customer in writing if it cannot comply with the requirements under Sections 5-8 of this DPA, in which case Customer may terminate the Agreement or take any other reasonable action, including suspending data processing operations;

b. Inform Customer promptly if, in LinkedIn's opinion, an instruction from Customer violates applicable Data Protection Requirements;

c. If LinkedIn is collecting Customer Personal Data from individuals on behalf of Customer, follow Customer's instructions regarding such Customer Personal Data collection (including with regard to the provision of notice and exercise of choice);

d. Take steps to ensure that (i) persons employed by it and (ii) other persons engaged to perform on LinkedIn's behalf comply with the terms of the Agreement;

e. Ensure that its employees, authorized agents and any Subprocessors are required to comply with and acknowledge and respect the confidentiality of the Customer Personal Data, including after the end of their respective employment, contract or assignment;

f. If it intends to engage Subprocessors to help it satisfy its obligations in accordance with this DPA or to delegate all or part of the processing activities to such Subprocessors, (i) exclusive of the list of Subprocessors LinkedIn and its Affiliates maintains online (currently available at https://legal.linkedin.com/customer-subprocessors), the use of which Customer approves, obtain the prior written consent of Customer to such subprocessing, such consent to not be unreasonably withheld; (ii) remain liable to Customer for the Subprocessors' acts and omissions with regard to data protection where such Subprocessors act on LinkedIn's instructions; and (iii) enter into contractual arrangements with such Subprocessors binding them to provide the same level of data protection and information security to that provided for herein; and

g. Upon request, provide Customer with a mapping of LinkedIn's security policies to the controls set forth in the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27001 standard.

5.2 Notice to Customer. LinkedIn will inform Customer if LinkedIn becomes aware of:

a. Any non-compliance by LinkedIn or its employees with Sections 5-8 of this DPA or the Data Protection Requirements relating to the protection of Customer Personal Data Processed under this DPA;

b. Any legally binding request for disclosure of Customer Personal Data by a law enforcement authority, unless LinkedIn is otherwise forbidden by law to inform Customer, for example to preserve the confidentiality of an investigation by law enforcement authorities;

c. Any notice, inquiry or investigation by a Supervisory Authority with respect to Customer Personal Data; or

d. Any complaint or request (in particular, requests for access, rectification, erasure, restriction, portability, blocking or deletion of Customer Personal Data) received directly from data subjects of Customer. LinkedIn will not substantively respond to any such request without Customer's prior written authorization.

5.3 Assistance to Customer. LinkedIn will provide reasonable assistance to Customer regarding:

a. Any requests from Customer data subjects in respect of access to or the rectification, erasure, restriction, portability, blocking or deletion of Customer Personal Data that LinkedIn Processes for Customer. In the event that a data subject sends such a request directly to LinkedIn, LinkedIn will promptly send such request to Customer;

b. The investigation of Personal Data Breaches and the notification to the Supervisory Authority and Customer's data subjects regarding such Personal Data Breaches; and

c. Where appropriate, the preparation of data protection impact assessments and, where necessary, carrying out consultations with any Supervisory Authority.

5.4 Required Processing. If LinkedIn is required by Data Protection Requirements to Process any Customer Personal Data for a reason other than providing the services described in the Agreement, LinkedIn will inform Customer of this requirement in advance of any Processing, unless LinkedIn is legally prohibited from informing Customer of such Processing (e.g., as a result of secrecy requirements that may exist under applicable EU member state laws).

5.5 Security. LinkedIn will:

a. Maintain appropriate organizational and technical security measures (which may include, with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, incident response, encryption of Customer Personal Data while in transit and at rest) designed to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Customer Personal Data, including the security measures set forth in Schedule D to this DPA, which shall apply as Annex II of the SCCs;

b. Be responsible for the sufficiency of the security, privacy, and confidentiality safeguards of all LinkedIn personnel with respect to Customer Personal Data and liable for any failure by such LinkedIn personnel to meet the terms of this DPA;

c. Take reasonable steps to confirm that all LinkedIn personnel are protecting the security, privacy and confidentiality of Customer Personal Data consistent with the requirements of this DPA, which shall apply as Annex II of the SCCs; and

d. Notify Customer of any Personal Data Breach by LinkedIn, its Subprocessors, or any other third parties acting on LinkedIn's behalf without undue delay and in any event within 48 hours of becoming aware of a Personal Data Breach.

e. If a Personal Data Breach results from either (i) the negligence or intentional misconduct of LinkedIn (or any LinkedIn Subprocessor consistent with Section 5.1(f)) or (ii) a material failure of LinkedIn to comply with the terms of this DPA, LinkedIn shall bear all costs associated with investigating and remediating the Personal Data Breach. LinkedIn shall provide reasonable reimbursement to Customer for any costs associated with notifying affected individuals as required by law or providing individuals with credit monitoring or other appropriate remediation services, provided that LinkedIn, as a processor, will adhere to its commitments under 5.3(b) of this DPA.

6. AUDIT, CERTIFICATION

6.1 Supervisory Authority Audit of Customer. If a Supervisory Authority requires an audit of the data processing facilities from which LinkedIn Processes Customer Personal Data in order to ascertain or monitor Customer's compliance with Data Protection Requirements, LinkedIn will cooperate with such audit. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time LinkedIn expends for any such audit, in addition to the rates for services performed by LinkedIn.

6.2 Audits. Upon request, LinkedIn will provide to Customer each year an opinion or Service Organization Control report provided by an accredited, third-party audit firm under the Statement on Standards for Attestation Engagements (SSAE) No. 18 ("**SSAE 18**") (Reporting on Controls at a Service Organization) or the International Standard on Assurance Engagements (ISAE) 3402 ("**ISAE 3402**") (Assurance Reports on Controls at a Service Organization) standards applicable to the services under the Agreement (each such report, a "**Report**"). If a Report does not provide, in Customer's reasonable judgment, sufficient information to confirm LinkedIn's compliance with the terms of this DPA, then Customer or an accredited third-party audit firm agreed to by both Customer and LinkedIn may audit LinkedIn's compliance with the terms of this DPA during regular business hours, with reasonable advance notice to LinkedIn and subject to reasonable confidentiality procedures. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time LinkedIn expends for any such audit, in addition to the rates for services performed by LinkedIn. Before the commencement of any such audit, Customer and LinkedIn shall mutually agree upon the scope, timing, and duration of the audit. Customer shall promptly notify LinkedIn with information regarding any non-compliance discovered during the course of an audit. Customer may not audit LinkedIn more than once annually.

7. DATA TRANSFERS

7.1 For transfers of EU Personal Data to LinkedIn for processing by LinkedIn in a jurisdiction other than a jurisdiction in the EU, the EEA, or the European Commission-approved countries providing 'adequate' data protection, each party agrees it will use Module 2 of the SCCs for Controller to Processor transfers, which are incorporated herein by reference. The parties agree that the following terms apply: (i) the Data Protection Commission of Ireland shall be the competent Supervisory Authority pursuant to Clause 13 of the SCCs; (ii) data subjects for whom a LinkedIn entity processes EU Personal Data are third-party beneficiaries under the applicable SCCs; (iii) the SCCs shall be governed by the law of Ireland, which allows for third-party beneficiary rights pursuant to Clause 17 of the SCCs; and (iv) any dispute arising from the SCCs shall be resolved by the courts of Ireland pursuant to Clause 18 of the SCCs. Schedule A to this DPA shall apply as Annex I of SCCs and Schedule D shall apply at Annex II of the SCCs.

7.2 If LinkedIn is unable or becomes unable to comply with these requirements, then EU Personal Data will be processed and used exclusively within the territory of a member state of the European Union and any movement of EU Personal Data to a non-EU country requires the prior written consent of Customer. LinkedIn shall promptly notify Customer of any inability by LinkedIn to comply with the provisions of this Section 7. Notwithstanding the foregoing, where the transfers contemplated under this Section 7 result in transfers of UK Personal Data to LinkedIn for processing by LinkedIn in a jurisdiction other than in the UK or UK Information Commissioner's Office-approved countries providing 'adequate' data protection, (1) each party agrees it will use the 2010 Controller-to-Processor SCCs for so long as such SCCs are lawfully permitted for such transfers of UK Personal Data, and (2) Schedules A and D shall apply as Annex I and Annex II, respectively. In the event that the UK Information Commissioner's Office confirms that a "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") is required to rely lawfully on the SCCs for transfers of UK Personal Data, then (a) the SCCs used for EU Personal Data shall also apply to transfers of UK Personal Data; (b) the UK Addendum shall be deemed executed between Customer and LinkedIn; and (c) the SCCs between the parties shall be deemed amended as specified in the UK Addendum in respect of the transfer of such UK Personal Data. The UK Information Commissioner is the exclusive Supervisory Authority for the transfers of UK Personal Data under this Agreement.

8. DATA RETURN AND DELETION

The parties agree that on the termination of the data processing services or upon Customer's reasonable request, LinkedIn shall, and shall cause any Subprocessors to, at the choice of Customer, return all the Customer Personal Data and copies of such data to Customer or securely destroy them and demonstrate to the satisfaction of Customer that it has taken such measures, unless Data Protection Requirements prevent LinkedIn from returning or destroying all or part of the Customer Personal Data disclosed. In such case, LinkedIn agrees to preserve the confidentiality of the Customer Personal Data retained by it and that it will only actively Process such Customer Personal Data after such date in order to comply with applicable laws. For clarity, LinkedIn may continue to Process Customer Personal Data that has been aggregated in a manner that does not identify individuals or customers to improve LinkedIn's systems and services.

9. CONTROLLER-TO-CONTROLLER SCENARIOS

Certain Services may offer integrated viewing and export of Personal Data of LinkedIn members that Customer already may access on LinkedIn's website, LinkedIn.com, consistent with member privacy settings. For purposes of GDPR, where there is a member-directed export of Personal Data or where Customer already may access such Personal Data, both Customer and LinkedIn will be independent controllers of Personal Data originally derived on the LinkedIn Services. The parties agree that, for such cases, LinkedIn and Customer would each act as a data controller with respect to their particular copy of the Personal Data. Each party will, to the extent that it, along with the other party, acts as data controller, as the term is defined in applicable Data Protection Requirements, with respect to Personal Data, reasonably cooperate with the other party to enable the exercise of data protection rights as set forth in the Data Protection Requirements. Where both parties each act as data controller with respect to Personal Data, and the transfer of data between the parties results in a transfer of EU Personal Data to a jurisdiction other than a jurisdiction in the EU, the EEA, or the European Commission-approved countries providing 'adequate' data protection, each party agrees it will use Module 1 of the SCCs, which are incorporated herein by reference. The parties agree that the following terms apply: (i) the Data Protection Commission of Ireland shall be the competent Supervisory Authority pursuant to Clause 13 of the SCCs; (ii) data subjects for whom a LinkedIn entity processes EU Personal Data are third-party beneficiaries under the applicable SCCs; (iii) the SCCs shall be governed by the law of Ireland, which allows for third-party beneficiary rights pursuant to Clause 17 of the SCCs; and (iv) any dispute arising from the SCCs shall be resolved by the courts of Ireland pursuant to Clause 18 of the SCCs. Notwithstanding the foregoing, where

the transfers contemplated under this Section 9 results in a transfer of UK Personal Data to a jurisdiction other than in the UK or UK Information Commissioner's Office-approved countries providing 'adequate' data protection, (1) the 2004 Controller-to-Controller SCCs, which are incorporated herein by reference, will apply for so long as such SCCs are lawfully permitted for such transfers of UK Personal Data, (2) Schedule A and Schedule D shall apply as Annex B and Annex II, respectively, and (3) for purpose of Section II(h), the data importer will process the UK Personal Data, at its option, in accordance with the data processing principles set out in Annex A of the Controller-to-Controller SCCs. In the event that the UK Information Commissioner's Office confirms that a UK Addendum is required to rely lawfully on the SCCs contemplated under this Section 9 for transfers of UK Personal Data, then (a) SCCs used for EU Personal Data under this Section 9 shall also apply to transfers of UK Personal Data; (b) the UK Addendum shall be deemed executed between Customer and LinkedIn; and (c) the SCCs between the parties shall be deemed amended as specified in the UK Addendum in respect of the transfer of such UK Personal Data..

Unless otherwise agreed in writing, the parties acknowledge and agree that each is acting independently as Data Controller with respect of Personal Data and the parties are not joint controllers as defined in the General Data Protection Regulation and UK GDPR.

10. THIRD PARTY DATA PROCESSORS

Customer acknowledges that in the provision of some services (such as Applicant Tracking Systems, Learning Management Systems, and Customer Management Systems), LinkedIn, on receipt of instructions from Customer, may transfer Customer Personal Data to and otherwise interact with third party data processors. Customer agrees that if and to the extent such transfers occur, Customer is responsible for entering into separate contractual arrangements with such third-party data processors binding them to comply with obligations in accordance with Data Protection Requirements. For avoidance of doubt, such third-party data processors are not Subprocessors.

11. TERM

This DPA shall remain in effect as long as LinkedIn carries out Personal Data processing operations on behalf of Customer or until the termination of the LinkedIn Contract (and all Personal Data has been returned or deleted in accordance with Section 8 above).

12. GOVERNING LAW, JURISDICTION, AND VENUE

Notwithstanding anything in the Agreement to the contrary, this DPA shall be governed by the laws of Ireland, and any action or proceeding related to this DPA (including those arising from non-contractual disputes or claims) will be brought in Dublin, Ireland. However, where a dispute arises regarding the processing of UK Personal Data under this DPA, such dispute shall be governed by the laws of England and Wales.

SCHEDULE A
ANNEX 1 - DESCRIPTION OF THE TRANSFER

Categories of data subjects whose Personal Data is transferred:

Module 1 (Controller to Controller): Registered users of LinkedIn.com ("LinkedIn Members")

Module 2 (Controller to Processor):

Categories of data subjects whose personal data is transferred

Services (As applicable)	**Categories of data subjects whose Personal Data is transferred:**
Talent/Hire	- Employees, contractors, partners and/or customers of data exporter - Potential and actual candidates of the data exporter - Third parties in the data exporter's Applicant Tracking System tool (typically this would be third parties that have, or may have, a relationship with the data exporter such as potential or actual candidates or employees)
Learning	- Employees, contractors, students, non-standard users (as individually approved by LinkedIn) and/or library patrons of data exporter
Glint/Engage	- Employees of data exporter - Third parties that have, or may have, a commercial relationship with the data exporter (e.g. contractors)
Sales Solutions	- Employees, contractors, partners and/or customers of data exporter

	- Third parties in the data exporter's Customer Relationship Management tool (typically this would be third parties that have, or may have, a commercial relationship with the data exporter such as customers and potential customers)
Marketing Solutions	- Employees, contractors, partners and/or customers of data exporter - LinkedIn members that engaged with the data exporter's properties or fall within the exporter's advertising audience

Categories of Personal Data transferred:

Module 1 (Controller to Controller)

The data transferred is the Personal Data of LinkedIn Members that Customer already may access on LinkedIn's website, LinkedIn.com, consistent with member privacy settings, provided by the data exporter (LinkedIn) to the data importer (Customer) in connection with Customer's use of LinkedIn's online recruiting, sales, and/or learning services, and subsequently processed by Customer for its own purposes. Such Personal Data may include first name, last name, email address, contact information, education, and work history.

Module 2 (Controller to Processor)

The data transferred is the Personal Data provided by the data exporter (Customer) to the data importer (LinkedIn) in connection with its use of LinkedIn's online recruiting, sales, marketing, employee engagement, and/or learning services, referred to as Customer Personal Data in the Data Processing Agreement.

Such Customer Personal Data may include, depending on the Customer's or Customer's seat holder's input/interaction

Such Customer Personal Data may include, depending on the Customer's or Customer

Services (As applicable)	**Categories of Customer Personal Data**
Talent/Hire	- Talent/Hire user information (may include name, email, title)

	- Job Postings (usage data of job post creator, applicant data, screening questions and answers) - Product usage data (including Hiring Projects, Recruiter messaging content, resumes uploaded as part of job application, notes on a candidate profile) - Applicant data (resume data, contact details and other profile information submitted as part of an application) - Usage reporting for Talent Solutions users - (If applicable) Recruiter Systems Connect (candidate status, application notices, action taken, stub profiles, InMail responses) - IP address, device/browser characteristics
Learning	- Learning user information (may include user ID, unique ID, name, email address) - (If applicable) Library card number + password - Product usage data (including learning activity, bookmarks, likes, notes and quiz results) - IP address, device/browser characteristics
Glint/Engage	- Personal information about its personnel (may include name, company-issued email address, employer-issued identification number, work location, job function, department code, employee grade level, birth year, binary gender,

	continuous service data, other personnel information in data exporter's human resource information system (HRIS); IP address, device/browser characteristics) - Enterprise Login Information (if using SSO) - Product usage data (including Survey respondent opinions provided in response to survey questions and employee-feedback provided in response to performance feedback questions).
Sales Solutions	- Sales Navigator user information - Product usage data (including InMail/Messages, Notes, Tags, SmartLinks presentations and user created contact details) - Usage Reporting for Sales Navigator User and - (If applicable) any CRM data synced to Sales Navigator - IP address, device/browser characteristics
Marketing Solutions	- Seat holder enterprise login and product usage data - (If applicable) CRM data - (If applicable) Sales and marketing leads

	- (If applicable) Matched Audience Contact Targeting Information including Hashed email address, First and last name, Employer, Job Title, Country, Mobile device IDs - (If applicable) Insight Tag Data, including member pseudonym, IP address, device and browser characteristics, time stamp, URL. - (If applicable) Advertising criteria received by LinkedIn Audience Networks via the Real Time Bidding process

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

No

If Yes, include a description of the applied restrictions or safeguards in place here:

N/A

The frequency of the transfers (e.g. whether the data is transferred on a one-off or continuous basis):

Continuous

Nature of the processing

Collection, organization, structuring, use, storage, combination, making available on LinkedIn properties in accordance with the relevant services.

Purpose(s) of the data transfer and further processing:

- Provide, maintain and improve services (in accordance with the DPA) to the data exporter,
- Provide customer support to the data exporter,
- Otherwise fulfil LinkedIn's (and, if applicable, its affiliate's) obligations under its respective services agreement with the data exporter; and
- Compliance with applicable law.

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:

LinkedIn will retain the data for the duration of the term of the services specified on the ordering document and in accordance with Section 8 of the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

LinkedIn uses sub-processors to support its infrastructure environment, local and international providers of telecommunications and networking services, legal entities engaged in data storage and content delivery material. Personal Data processed by sub-processors is processed for the purposes and duration of the relevant LinkedIn services agreement or ordering document. For more information, see LinkedIn's List of Subprocessors located at the following web address: https://legal.linkedin.com/customer-subprocessors, which also shall apply as Annex III of the SCCs, where applicable.

Miscellaneous

For Hire, Learning, and Sales, the Personal Data of LinkedIn Members who are Customer's users and who choose to connect their personal LinkedIn.com Member profile with the enterprise seat provided by the Customer is not included herein and is governed instead by the separate Standard Contractual Clauses between LinkedIn Ireland Unlimited Company as data exporter and LinkedIn Corporation as the data importer.

SCHEDULE B
ADDENDUM TO LINKEDIN DATA PROCESSING AGREEMENT
California Consumer Privacy Act

This Addendum is entered into by the LinkedIn customer identified on the applicable LinkedIn ordering document for LinkedIn services ("Customer") and the LinkedIn company identified on the ordering document ("LinkedIn"), and amends the LinkedIn Data Processing Agreement between Customer and LinkedIn ("DPA") with respect to LinkedIn's processing of Customer Personal Data of California Consumers under the CCPA. Capitalized terms used but not otherwise defined in this Addendum will have the meanings given to them in the DPA. Capitalized terms not otherwise defined in the DPA, will have the meanings given to them under the CCPA.

No CCPA Sale. The parties agree that for the purposes of the CCPA, LinkedIn acts as a CCPA Service Provider for Customer Personal Data. By executing the ordering document,

- Customer does not Sell Customer Personal Data to LinkedIn. LinkedIn shall only use Customer Personal Data for the purposes permitted by the CCPA and as specified in the Agreement. LinkedIn agrees not to Sell or Share (as defined by the CCPA) Customer Personal Data.
- LinkedIn agrees not to combine Customer Personal Data with other personal information except as permitted by the CCPA.
- To the extent LinkedIn receives information from Customer that has been deidentified, as defined under applicable Data Protection Requirements, LinkedIn agrees not to attempt to reidentify the data, to take reasonable measures to maintain and use the information in a deidentified manner, except as permitted by law, and to contractually obligate any authorized recipients to comply with applicable Data Protection Requirements for information that has been deidentified.
- LinkedIn agrees to inform Customer within the time period required under the CCPA, if LinkedIn determines that it is no longer able to meet its obligations under the CCPA.
- LinkedIn certifies that it has read and understands this Addendum and will abide by it, including by avoiding any action that would cause the other Party to be deemed to have Sold Personal Data or Personal Information under the CCPA.

SCHEDULE C
GLINT-SPECIFIC TERMS AND AMENDMENTS

The following terms and conditions amend the DPA with respect to only those LinkedIn products and services offered under the Glint brand (including Glint Engage and Glint Perform). For avoidance of doubt, if Customer purchases Glint services as provided under the Agreement ("Glint Services") in addition to LinkedIn-branded services, the following amendments apply only with respect to those Glint products or services and the DPA will apply unamended with respect to the LinkedIn-branded services.

The following clauses are added to the DPA as a new Section 4.3:

4.3 Notice and Choice.

a. Customer agrees to provide appropriate notices to its Customer Users of the Glint Services about and, if required by Data Protection Requirements, obtain appropriate consent or other appropriate legal basis from such Customer Users for: (i) the collection, transfer and processing of Customer Personal Data through LinkedIn's services and (ii) Customer's use of any service providers or other third-parties that Customer instructs LinkedIn to send Customer Personal Data to or provide Customer Personal Data to LinkedIn. Without limiting the generality of the foregoing, Customer may provide LinkedIn with Personal Data for the purpose of enabling LinkedIn to provide the LinkedIn services. Customer represents and warrants that it has the necessary right and full power and authority to provide the Personal Data to LinkedIn.

b. Customer will decide the content of "User Confidentiality Notices" that will be provided to Customer Users (e.g., for Glint Engage, a survey Confidentiality Notice) relating to the degree of confidentiality and aggregation threshold that a Customer User will have and, if applicable, any required disclosures under any Data Protection Requirement (e.g., Art. 13 of the General Data Protection Regulation). At Customer's option, Customer may use a default LinkedIn User Confidentiality Notice. Customer's Master Admin will provide LinkedIn with the User Confidentiality Notice at least three (3) business days prior to use. Customer agrees that it will not modify or delete any portion of the User Confidentiality Notice or include any statements in any communication with a Customer User that imposes any obligation on LinkedIn or in any way modifies, contradicts, or supplements User Confidentiality Notice provided to LinkedIn. Customer is solely and exclusively responsible for ensuring that its use of Customer Personal Data and the User Confidentiality Notice complies with all applicable Data Protection Requirements.

The following clauses are added to the DPA as a new Section 4.4:

4.4 Aggregation and Non-Identification. To the extent a User Confidentiality Notice informs Customer Users that the Customer will only receive data from LinkedIn in an aggregated form, Customer agrees it will not receive, nor attempt to discern, any such Customer Personal Data in a form that identifies individual Customer Users with Customer Personal Data.

The first sentence of Section 5.1.a of the DPA is replaced with the following sentence:

Process Customer Personal Data (i) only for the purpose of providing, supporting and improving the Glint Services (including by providing aggregated, non-identifiable insights to improve the Glint Services and LinkedIn services, and providing survey benchmarking data to LinkedIn customers, where both the data subject and Customer have been de-identified), using appropriate technical and organizational security measures; and (ii) in compliance with the instructions received from Customer.

Section 5.1.g of the DPA is replaced in its entirety with the following clause:

Upon request, provide Customer with a summary of LinkedIn's security policies applicable to the Glint-branded services.

Section 8 of the DPA is replaced in its entirety with the following clauses:

The parties agree that on the termination of the data processing services, LinkedIn shall, and shall cause any Subprocessors to, at the choice of Customer, unless Data Protection Requirements prevent LinkedIn from returning or destroying all or part of the Customer Personal Data disclosed: (i) return to Customer all the Customer Personal Data, including survey responses if the Customer User Confidentiality Notice disclosed Customer would receive responses identified to individuals, or (ii) securely destroy them and demonstrate to the satisfaction of Customer that it has taken such measures or (iii) export Customer Personal Data in a non-aggregated form to Customer's new service provider under a separate written agreement reasonably satisfactory to LinkedIn under which Customer and the recipient of the data accept responsibility and liability for the Customer Personal Data subsequent to transfer or export. LinkedIn agrees to preserve the confidentiality of the Customer Personal Data retained by it and that it will only actively process such Customer Personal Data after such date in order to comply with applicable Data Protection Requirements. For clarity, after termination of the LinkedIn Contract, LinkedIn may continue to process Customer Personal Data that has been aggregated in a manner that does not identify individuals or customers to improve LinkedIn's systems and services.

Sections 9 and 10 of the DPA will not apply in the context of Glint products or services.

SCHEDULE D
Annex II to the SCCs
TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. General Security Measures

Data Importer will comply with industry standard security measures (including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, and incident response measures necessary to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Data Exporter's Personal Data provided by Data Exporter to Data Importer), as well as with all applicable data privacy and security laws, regulations and standards.

2. Contact Information

Data Importer's security team can be reached at security@linkedin.com for any security issues or questions related to the product.

3. Compliance

Data Importer complies with the standards and practices set forth at the following web address: https://security.linkedin.com/trust-and-compliance. Data Exporter must contact their LinkedIn account manager for any additional information on the security certifications listed at the web address.

4. Information Security Program

The objective of LinkedIn Information Security Program is to maintain the confidentiality, integrity and availability of its computer and data communication systems while meeting necessary legislative, industry, and contractual requirements. Data Importer shall establish, implement, and maintain an information security program that includes technical and organizational security and physical measures as well as policies and procedures to protect Data Exporter data processed by Data Importer against accidental loss; destruction or alteration; unauthorized disclosure or access; or unlawful destruction.

4.1 Secure Software Development

Data Importer shall maintain policies and procedures to ensure that system, device, application and infrastructure development is performed in a secure manner. This includes review and test of all Data Importer applications, products and services for common security vulnerabilities and defects, employing defense-in-depth strategy through the use of multiple layers of security boundaries and technologies, periodic pen testing and security assessment of these services, defining baseline configurations and requirements for patching of third party systems.

4.2 Human Resources Security

Data Importer shall maintain a policy which defines requirements around enforcing security measures as they relate to employment status changes. This includes background checks, acknowledgement and adherence to Data Importer's security policies, onboarding and termination for employees and third parties.

4.3 Data Classification & Protection

Data Importer shall maintain policies and procedures for data classification and protection, along with requirements for classification of data containing Personal Data in consideration of applicable laws, regulations and contractual obligations. Data Importer shall also maintain requirements on data encryption, rules for transmission of data and requirements for removable media, along with requirements on how access to these data should be governed.

4.4 Network Security

Data Importer shall maintain policies and procedures around the network infrastructure used to process Data Exporter data, establish and enforce safe network practices, and define service level agreements with internal and external network services.

4.5 Physical and Environmental Security

Data Importer shall maintain policies and procedures for physical and environmental security, define requirements to protect areas that contain sensitive information and ensure that critical information services be protected from interception, interference or damage.

4.6 Business Continuity and Disaster Recovery

Data Importer shall maintain policies and procedures to ensure that Data Importer may continue to perform business critical functions in the face of an extraordinary event. This includes data center resiliency and disaster recovery procedures for business-critical data and processing functions.

5. Access Control

Data Importer shall maintain access control measures designed to limit access to Data Importer's facilities, applications, systems, network devices and operating systems to a limited number of personnel who have a business need for such access. Data Importer shall ensure such access is removed when no longer required and shall conduct access reviews periodically.

6. Risk Assessments

Data Importer has a documented risk management procedure and Secure Software Development LifeCycle process. Data Importer performs risk assessments of its products and infrastructure on a regular basis, including review of the data classification policies and targeted reviews of highly sensitive data flows.

Data Importer performs application and infrastructure level testing for every new product that is launched as well as periodic reassessments of its network, as well as feature changes. Data Importer leverages access control, and peer code review which would ensure that viruses are not introduced in the code and detect such abuse. Data Importer uses a combination of manual penetration testing and automated tools.

7. Third-Party Risk Assessments

Data Importer conducts security due diligence on third-party service providers to assess and monitor risk. This assessment includes a review of scope of confidential information and personal data transferred to or processed by the service provider and the purpose of the work. Data Importer will also conduct a risk assessment which may include the service provider’s organization and technical security measures, the

sensitivity of any information processed by the service provider, storage limitations, and data deletion procedures and timelines.

8. Supplementary Measures

In addition to the general security measures set out above, the Data Importer has implemented the following supplementary technical and organisational measures:

- Customer Personal Data as defined in the Data Processing Agreement is transferred across public networks to the Data Importer's data centres in the United States and is stored on secured servers behind firewall.
- New Glint Customers may select between the Glint US or Glint EU data storage locations for hosting of their Glint-specific Customer Personal Data.
- Data Importer encrypts all Customer Personal Data in transit across public networks depending on the Data Exporter's ability to support encryption. Certain highly confidential data (including but not limited to passwords, authentication tokens, salary and payment information) is also encrypted at rest. LinkedIn will only use industry tested and accepted standards for cryptographic algorithms.
- Data Importer's data is replicated across all its data centres in a secure environment.
- Data Importer employs app logic with appropriate authorization to protect tenant data. Access requests are reviewed to ensure only appropriate access is granted. Server and database access logs are retained for auditing purposes.
- Data Importer deploys industry standard security measures for all of its product lines as further set forth at https://security.linkedin.com/trust-and-compliance, including 27001 & ISO 27018 and PCI DSS for Data Importer's Talent Solutions, Learning Solutions, Marketing Solutions and Sales Solutions. Data Importers' employees and contractors are trained in relation to specific technical and organisational security measures.
- Servers are monitored by both industry standard and proprietary network monitoring tools to prevent any potential security breaches.
- Corporate systems and databases are password protected.
- VPN and direct LinkedIn network access are limited to company issued or approved devices.
- Dual factor authentication is in operation for VPN access.
- Customer and member passwords are hashed and salted and stored in a separate, secure database.
- Keys to credit card database are rotated regularly.
- Active and automated monitoring of critical access logs and anomaly detection.