Syntel Human Resources Privacy Statement

Date of Modification (dd/mm/yy)	Resulting Version #	Modifications Made
24th August 2016	1.0	Base Version
13th March 2018	2.0	Modification to comply Privacy Shield requirements
22nd May 2018	3.0	Modifications to cover usage of online media for corporate purpose.

Privacy Statement highlights:

Syntel is committed to protecting your privacy. This Privacy Statement ("Statement") addresses prospective, current, and former members of Syntel's workforce and explains how Syntel uses and protects the data we collect about current and prospective employees throughout the course of the employment relationship, including via our online job portal. In this context, this Statement applies to any personal data you provide to Syntel and, subject to local law, any personal data about you that we collect from other sources.

Throughout this Statement, "Syntel" refers to Syntel Europe Ltd, including its affiliated companies and subsidiaries as mentioned below (also referred to as "we", "us", or "our").

	SYNTEL EUROPE ENTITIES
1.	Syntel Europe Limited (UK)
2.	Syntel Deutschland GmbH (Germany)
3.	Syntel Solutions BV (Netherlands)
4.	Syntel Switzerland GmbH
5.	Intellisourcing SARL (Paris)
6.	Syntel Poland Sp. z o.o
	SYNTEL US ENTITIES
1.	Syntel, Inc.

EU-U.S. and Swiss-U.S. Privacy Shield Frameworks

With respect to personal data processed in Syntel's human resources management systems, such as Peoplesoft HRMS and Hirecraft, Syntel, Inc. of the United States complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework (the "Privacy Shield") as adopted and set forth by the U.S. Department of

Commerce regarding the processing of personal data. Syntel, Inc. commits to adhere to and has certified to the Department of Commerce that it adheres to the Privacy Shield Principles.

To learn more about the Privacy Shield, and to view Syntel, Inc.'s certification, please visit https://www.privacyshield.gov and https://www.privacyshield.gov/list, respectively.

VeraSafe Privacy Program

Syntel, Inc. is a member of the VeraSafe Privacy Program, meaning that with respect to personal data processed in the scope of this Statement, VeraSafe has assessed Syntel Inc.'s data governance and data security for compliance with the VeraSafe Privacy Program Certification Criteria. The certification criteria require that participants maintain a high standard for data privacy and implement specific best practices pertaining to notice, onward transfer, choice, access, data security, data quality, recourse, and enforcement.

Dispute Resolution

Within the scope of Syntel, Inc.'s Privacy Shield certification, where a privacy complaint or dispute cannot be resolved through Syntel, Inc.'s internal processes, Syntel, Inc. has agreed to participate in the VeraSafe Privacy Shield Dispute Resolution Procedure. Subject to the terms of the VeraSafe Privacy Shield Dispute Resolution Procedure, VeraSafe will provide appropriate recourse free of charge to you. To file a complaint with VeraSafe and participate in the VeraSafe Privacy Shield Dispute Resolution Procedure, please submit the required information here: https://www.verasafe.com/privacy-services/dispute-resolution/submit-dispute/

If a complaint or dispute cannot be resolved through Syntel, Inc.'s internal process, nor through the dispute resolution program established by VeraSafe, Syntel, Inc. has agreed to cooperate with the EU data protection authorities and the Swiss Federal Data Protection and Information Commissioner and to participate in the dispute resolution procedures of the panel established by such data protection authorities.

Controllership

In the context of this Statement, Syntel's various entities act as joint controllers for the data processed by those entities.

Basis of Processing

Within the scope of this Statement, we process personal data on the basis of your consent in cases where you are not a current or former employee of Syntel, the need to perform our obligations under an employment contract we have entered into with you, or to perform related pre-contractual duties at your request, the necessity to comply with our legal obligations, such as to share certain personal data with tax authorities. Where none of the aforementioned is applicable, Syntel processes your personal data on the basis of our legitimate interests, such as the need to facilitate communication between Syntel's multinational group of companies.

What type of information does Syntel collect?

If you deal with Syntel in your private capacity (which does not include employees, temporary workers or other personnel of Syntel), for example if you take part in Syntel recruitment, we typically process the following types of personal data about you:

- Biographical information, such as name, date of birth, occupation, marital status, country of residence, and national insurance number, or equivalent.
- Professional and personal contact information, such as email address, postal address and/or telephone number.
- Employment records, such as professional membership, references, and proof of eligibility to work in the local jurisdiction.
- Identification documentation, such as a photocopy of your passport, driving license, ID card or other documentation required by local law. Such copies may include a photograph of your face and shoulders.
- Other information provided by you in our recruitment process.
- Details of your visit(s) to our premises.

If you deal with Syntel in your capacity as an employee, temporary worker or other personnel, we typically process the following types of personal data about you:

- Biographical and personal contact information, such as name, address, date of birth, gender, marital status, race, ethnicity, emergency contact details, country of residence, national insurance number, salary, pension details, and bank/financial details.
- Professional details, such as email address, postal address, telephone number, your CV, qualifications, relevant experience and skills.
- Employment records, such as professional membership, trade union membership.
- References, and proof of eligibility to work in the local jurisdiction.
- Identification documentation, such as a photocopy of your passport, driving license, ID card or other documentation required by local law. Such copies may include a photograph of your face and shoulders.
- HR related records, such as training, performance assessments, absence and time-keeping records, disciplinary, grievance or culpability proceedings, employment tribunal applications, complaints, accidents, and incident details and results of background checks.
- Details of your access to our premises and to systems, software, and applications including access and location data and communications data.
- Information in relation to life, health and safety.
- Offences (including alleged offences), criminal proceedings, outcomes and sentences.
- Workers compensation insurance.
- Employee benefit programs.

When you provide us with this personal data, you understand and give your explicit consent that we may collect, use, and disclose this information to appropriate third parties for the purposes described in this Statement. Such personal data may include sensitive personal data.

We may also store emails, and application and Internet logs in connection with your dealings with us.

In certain circumstances it may be mandatory for you to provide us with your personal data to enable us to perform our obligations pursuant to an employment contract or other agreement entered into between you and us, or to comply with our legal obligations. In other circumstances, it will be at your discretion whether or not you provide us with personal data. However, failure to supply any of the personal data we request may mean that we are unable to maintain or provide services to you or your employer and/or you may be unable to take part in any of our recruitment campaigns, or fully access and use our internal systems and resources.

Syntel makes reasonable efforts to maintain the accuracy and completeness of your personal data that it stores and to ensure all of your personal data is up to date. However, you can assist us with this considerably by promptly contacting us if there are any changes to your personal data or if you become aware that we have inaccurate personal data relating to you. (See section below 'Your rights in relation to the personal data we collect.') Syntel shall not be responsible for any losses arising from any inaccurate, inauthentic, deficient or incomplete personal data or sensitive personal data that you provide to us.

How we collect your personal data

Syntel usually collects your personal data during the course of your, or your employer's, relationship with us. This will typically be through the forms and documents used when you sign up to our websites, take part in a recruitment campaign as a prospective candidate, or when you become an employee, contractor, temporary worker or other personnel. Additionally, your personal data will be collected during employee performance assessments and reviews, as described below in the Section 'What we use your personal data for'. We will also collect personal data when we monitor or record communications such as when you use Syntel-hosted technology including the PeopleSoft HRMS.

What we use your personal data for

Syntel and/or persons acting on our behalf may process your personal data for any of the following purposes, depending on the capacity in which you deal with Syntel:

- to ensure the content on applications is presented in the most effective manner for you;
- for general HR administration, including payroll and benefits management, training and development, performance management, health, sickness and absence management, grievance and disciplinary procedures, equal opportunities monitoring, business continuity planning;
- for internal finance management, including personnel expense reimbursement, travel and time-keeping;
- for monitoring and assessing compliance with Syntel's policies and standards;
- for our promotional and marketing materials and activities, including photos and videos;
- to carry out money laundering, financial and credit checks and for fraud and crime prevention and detection purposes;
- to provide you with requested services;
- to identify persons authorized for a selection process on behalf of our clients;
- for administrative purposes in relation to the security of and access to our systems, premises, platforms and secured websites and applications;
- to send you official communications;
- to consider your suitability for any of our current or future employment opportunities and to confirm your references and educational background;
- to comply with our legal and regulatory obligations and requests anywhere in the world, including reporting to and/or being audited by national and international regulatory, enforcement or exchange bodies; and
- to comply with court orders and exercise and/ or defend our legal rights.
- To provide information in response to request made by you via WhatsApp messenger service or other similar supported services. Your telephone number may be shared with the service while providing such information.

To whom we may disclose your personal data

Syntel does not and will not sell, rent or trade your personal data. We will only disclose your personal data in the ways set out in this Statement, including in the following circumstances:

- To any entity within the Syntel group where we have a legitimate interest in such transfer (which means any entity that's subsidiary to the Syntel, Inc.).
- To third parties who process your personal data on our behalf (such as our systems providers, or employee payroll provider).
- To third parties who process your personal data on their own behalf for the purpose of providing us or you with a service on behalf of us (such as our industry event organizers, or our employee pensions providers).
- To third parties in the course of offering or providing services to you. For example, settlement agents and HR consultants.
- To other financial institutions or regulatory bodies with whom information is shared for money laundering checks, credit risk reduction and other fraud and crime prevention purposes.
- To any third party to whom we assign or transfer any of our rights or obligations.
- To any prospective buyer in the event we sell any part of our business or its assets or if substantially all of our assets are acquired by a third party, in which case your personal data could form part of the assets we sell.
- To any national and/or international regulatory, enforcement or exchange body or court where we are required to do so by applicable law or regulation or at their request. (Please note that in such cases, Syntel may not be able to ensure that such recipient parties will provide adequate protection for your personal data.)
- To any central or local government department and other statutory or public bodies (such as Her Majesty's Revenue and Customs).
- To Syntel's clients for their operational purpose.

- To third parties operating communication channel or service over which Syntel provides information in response to your request.

When Syntel transfers your personal data to service providers, those service providers are contractually bound to maintain the confidentiality of such personal data and may not use the data for any unauthorized purpose. Syntel remains liable for the protection of your personal data that we transfer to our service providers, except to the extent that we are not responsible for the event giving rise to any unauthorized or improper processing.

Syntel may transfer your personal data across geographies:

Syntel may transfer your personal data across national borders to Syntel entities or service providers in other countries working on our behalf in accordance with applicable law. This may include transfers to jurisdictions that may not have data privacy laws providing equivalent protection to the laws in your home country.

If you are not a current or former employee of any Syntel entity, then whenever you provide your personal data to Syntel, you are explicitly giving us your duly informed and freely-given consent for Syntel to process your personal data in accordance with this Statement, including an authorization for Syntel to transfer data to group companies and service providers, some of whom are located in foreign countries.

Your rights in relation to the personal data we collect

If you wish to update or modify any of your personal data we store, access a copy of such personal data, or you would like us to stop processing any of your personal data which we hold and delete it, subject to local statutory regulations you can make such a request by writing to us at the address set out below. Subject to applicable law, we will process your request within the time prescribed by applicable law, not exceeding 30 days.

In any of the situations listed above, in order for us to comply with our data security obligations, we may request that you prove your identity by providing us with a copy of a valid means of identification.

You may also be able to view, update or modify certain elements of your personal data via the HR portal, accessible on our intranet.

How long we will hold your data for

We will only retain your personal data for as long as necessary to fulfill the purpose(s) for which it was collected or to comply with legal, regulatory or internal policy requirements. After such time, your personal data that we process will be destroyed. However, if you wish to have your personal data removed from our records, you can make such a request by writing to the address set out below subject to any legal, regulatory or internal policy requirements, we will then delete such data.

You may also be able to remove certain elements of your personal data via the HR portal, accessible on our intranet (subject to any legal, regulatory, or internal policy requirements).

How we protect your personal data and where we store it

Syntel is committed to safeguarding and protecting your personal data and maintains reasonable and appropriate security controls to protect any personal data you provide to us from improper or accidental disclosure, use, access, loss, modification or damage.

Occasionally, the personal data we collect from you may be processed in (including accessed in or stored in) a country or territory outside your home country, including outside the European Economic Area (“EEA”), which does not offer the same level of protection of personal data as may be enjoyed within your EEA home country. By submitting your personal data to us, you agree to this processing.

We will take all steps reasonably necessary to ensure that your personal data is appropriately protected and processed in accordance with applicable law and regulation and with Syntel’s policies and standards.

How we update or change this Privacy Statement

We may change or update this Statement in order to maintain our compliance with applicable law and regulation or following an update to our internal practices. We will do this by updating the wording on this webpage and updating the publication date at the top of this page. Please be aware that you will not necessarily be directly notified of such changes. Therefore, please ensure that you regularly check this Statement so you are fully aware of any changes or updates.

How you can contact us

If you would like to contact us in relation to this Statement or anything else in connection with your personal data that we process, including, without limitation, where you would like to update your personal data, would like a copy of your personal data that we process, or would like to raise a complaint or send a comment, please contact us using the details set out below.

In the UK:

Email: EUROPE_HRSUPPORT@Syntelinc.com
The Human Resources Officer, SYNTEL EUROPE LTD., Bolsover House, 5 Clipstone Street, London W1W 6BB, United Kingdom
Tel: +44 (O) 207 636 3587
Fax: +44 (O) 207 636 5975

In any other country:

Please contact your normal Human Resource representative and Information Security Team at Info_security@syntelinc.com, and explain that your communication is in relation to data protection.

On average we will respond to your data protection complaints/ grievances in approximately 5 working days; however, it may take up to 30 days depending on the complexity of your complaint/ grievance.

Binding Arbitration

With regards to data transferred to Syntel, Inc. in reliance on the Privacy Shield, if your dispute or complaint with Syntel, Inc. can't be resolved by us, nor through the dispute resolution program established by VeraSafe, or the dispute resolution panel of the EU data protection authorities, or the Swiss Federal Data Protection and Information Commissioner, as applicable, you may have the right to require that we enter into binding arbitration with you pursuant to the Privacy Shield's Recourse, Enforcement and Liability Principle and Annex I of the Privacy Shield.

Regulatory Oversight

Syntel, Inc. is subject to the investigatory and enforcement powers of the United States Federal Trade Commission.

You may also have a right to lodge your complaint with the supervisory authority, which is the data protection agency in your local European Union jurisdiction, or with the Swiss Data Protection and Information Commissioner. Syntel is subject to the investigatory and enforcement powers of such supervisory authority (ies).