ALLEGATO

"Accordo per il trattamento di dati personali"

1. Premesse

Il presente accordo costituisce allegato parte integrante del contratto/convenzione siglato/a tra il Committente e LepidaScpA, designata Responsabile del trattamento di dati personali ai sensi dell'art. 28 del Regolamento (UE) n. 2016/679 - GDPR.

Il presente Accordo si compone delle clausole di seguito rappresentate e dall'Allegato 1: Glossario

Le Parti convengono quanto segue:

2. Trattamento dei dati nel rispetto delle istruzioni del Committente

2.1 LepidaScpA, relativamente a tutti i Dati personali che tratta per conto del Committente garantisce che:

2.1.1 tratta tali Dati personali solo ai fini dell'esecuzione dell'oggetto del contratto, e, successivamente, solo nel rispetto di quanto eventualmente concordato dalle Parti per iscritto, agendo pertanto, esclusivamente sulla base delle istruzioni documentate e fornite dal Committente;

2.1.2 non trasferisce i Dati personali a soggetti terzi, se non nel rispetto delle condizioni di liceità assolte dal Committente e a fronte di quanto disciplinato nel presente accordo;

2.1.3 non tratta o utilizza i Dati personali per finalità diverse da quelle per cui è conferito incarico dal Committente, financo per trattamenti aventi finalità compatibili con quelle originarie;

2.1.4 prima di iniziare ogni trattamento e, ove occorra, in qualsiasi altro momento, informerà il Committente se, a suo parere, una qualsiasi istruzione fornita dal Committente si ponga in violazione di Normativa applicabile;

2.2 Al fine di dare seguito alle eventuali richieste da parte di soggetti interessati, LepidaScpA si obbliga ad adottare:

2.2.1 procedure idonee a garantire il rispetto dei diritti e delle richieste formulate al Committente dagli interessati relativamente ai loro dati personali;

2.2.2 procedure atte a garantire l'aggiornamento, la modifica e la correzione, su richiesta del Committente dei dati personali di ogni interessato;

2.2.3 procedure atte a garantire la cancellazione o il blocco dell'accesso ai dati personali a richiesta del Committente;

release: 100
data: 05.02.2019
redazione documento: Chiara Bonora e Licia Laghi
verifica documento: Gino Falvo, Lorenzo Fabbricatore
approvazione documento: Gianluca Mazzini

2.2.4 procedure atte a garantire il diritto degli interessati alla limitazione di trattamento, su richiesta del Committente.

2.3 Il Responsabile del trattamento deve garantire e fornire al Committente cooperazione, assistenza e le informazioni che potrebbero essere ragionevolmente richieste dalla stessa, per consentirle di adempiere ai propri obblighi ai sensi della normativa applicabile, ivi compresi i provvedimenti e le specifiche decisioni del Garante per la protezione dei dati personali.

2.4 Il Responsabile del trattamento, anche nel rispetto di quanto previsto all'art. 30 del Regolamento, deve mantenere e compilare e rendere disponibile a richiesta della stessa, un registro dei trattamenti dati personali che riporti tutte le informazioni richieste dalla norma.

2.5 Il Responsabile del trattamento assicura la massima collaborazione al fine dell'esperimento delle valutazioni di impatto ex art. 35 del GDPR che il Committente intenderà esperire sui trattamenti che rivelano, a Suo insindacabile giudizio, un rischio elevato per i diritti e le libertà delle persone fisiche.

3. Le misure di sicurezza

3.1 Il Responsabile del trattamento deve conservare i dati personali garantendo la separazione di tipo logico dei dati personali trattati per conto di terze parti o per proprio conto.

3.2 Il Responsabile del trattamento deve adottare e mantenere appropriate misure di sicurezza, sia tecniche che organizzative, per proteggere i dati personali da eventuali distruzioni o perdite di natura illecita o accidentale, danni, alterazioni, divulgazioni o accessi non autorizzati, ed in particolare, laddove il trattamento comporti trasmissioni di dati su una rete, da qualsiasi altra forma illecita di trattamento.

3.3. Il Responsabile del trattamento conserva, nel caso siano allo stesso affidati servizi di amministrazione di sistema, direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;

3.4 L'Ente attribuisce al Responsabile del trattamento il compito di dare attuazione alla prescrizione di cui al punto 2 lettera e) "Verifica delle attività" del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";

3.5 Il Responsabile del trattamento deve adottare misure tecniche ed organizzative adeguate per salvaguardare la sicurezza di qualsiasi rete di comunicazione elettronica o dei servizi forniti al Committente, con specifico riferimento alle misure intese a prevenire l'intercettazione di comunicazioni o l'accesso non autorizzato a qualsiasi computer o sistema.

release: 100
data: 05.02.2019
redazione documento: Chiara Bonora e Licia Laghi
verifica documento: Gino Falvo, Lorenzo Fabbricatore
approvazione documento: Gianluca Mazzini

4. Analisi dei rischi, privacy by design e privacy by default

4.1 Con riferimento agli esiti dell'analisi dei rischi effettuata dal Committente sui trattamenti di dati personali cui concorre LepidaScpA, lo stesso assicura massima cooperazione e assistenza al fine di dare effettività alle azioni di mitigazione previste dal Committente per affrontare eventuali rischi identificati.

4.2 LepidaScpA dovrà consentire al Committente, tenuto conto dello stato della tecnica, dei costi, della natura, dell'ambito e della finalità del relativo trattamento, di adottare, sia nella fase iniziale di determinazione dei mezzi di trattamento, che durante il trattamento stesso, ogni misura tecnica ed organizzativa che si riterrà opportuna per garantire ed attuare i principi previsti in materia di protezione dati e a tutelare i diritti degli interessati.

4.3 In linea con i principi di privacy by default, dovranno essere trattati, per impostazione predefinita, esclusivamente quei dati personali necessari per ogni specifica finalità del trattamento, e che in particolare non siano accessibili dati personali ad un numero indefinito di soggetti senza l'intervento di una persona fisica.

4.4 Il Responsabile del trattamento dà esecuzione al contratto in aderenza alle policy di privacy by design e by default adottate dal Committente e specificatamente comunicate.

5. Soggetti autorizzati ad effettuare i trattamenti – Designazione

5.1 Il Responsabile del trattamento garantisce competenze ed affidabilità dei propri dipendenti e collaboratori autorizzati al trattamento dei dati personali (di seguito anche incaricati) effettuati per conto del Committente.

5.2 Il Responsabile del trattamento garantisce che gli incaricati abbiano ricevuto adeguata formazione in materia di protezione dei dati personali e sicurezza informatica.

5.3 Il Responsabile del trattamento, con riferimento alla protezione e gestione dei dati personali, impone ai propri incaricati obblighi di riservatezza non meno onerosi di quelli previsti nel Contratto di cui il presente documento costituisce parte integrante. In ogni caso LepidaScpA è direttamente ritenuta responsabile per qualsiasi divulgazione di dati personali dovesse realizzarsi ad opera di tali soggetti.

6. Sub-Responsabili del trattamento di dati personali

6.1 Nell'ambito dell'esecuzione del contratto, LepidaScpA è autorizzata sin d'ora, alla designazione di altri responsabili del trattamento (d'ora in poi anche "sub-responsabili"), previa informazione del

Committente ed imponendo agli stessi condizioni vincolanti in materia di trattamento dei dati personali non meno onerose di quelle contenute nel presente Accordo.

6.2 Su specifica richiesta del Committente, LepidaScpA dovrà provvedere a che ogni SubResponsabile sottoscriva direttamente con il Committente un accordo di trattamento dei dati che, a meno di ulteriori e specifiche esigenze, preveda sostanzialmente gli stessi termini del presente Accordo.

6.3 In tutti i casi, LepidaScpA si assume la responsabilità nei confronti del Committente per qualsiasi violazione od omissione realizzati da un Sub-Responsabile o da altri terzi soggetti incaricati dallo stesso, indipendentemente dal fatto che LepidaScpA abbia o meno rispettato i propri obblighi contrattuali, ivi comprese le conseguenze patrimoniali derivanti da tali violazioni od omissioni.

7. Trattamento dei dati personali al di fuori dell'area economica europea

7.1 Il Committente non autorizza il trasferimento dei dati personali oggetto di trattamento al di fuori dell'Unione Europea.

8. Cancellazione dei dati personali

8.1 LepidaScpA provvede alla cancellazione dei dati personali trattati per l'esecuzione del presente contratto al termine del periodo di conservazione e in qualsiasi circostanza in cui sia richiesto dal Committente, compresa l'ipotesi in cui la stessa debba avvenire per dare seguito a specifica richiesta da parte di interessati.

8.2 Alla cessazione del Contratto e, conseguentemente del presente Accordo, per qualsiasi causa avvenga, i dati personali dovranno, a discrezione del Committente, essere distrutti o restituiti alla stessa, unitamente a qualsiasi supporto fisico o documento contenente dati personali di proprietà del Committente.

9. Audit

9.1 LepidaScpA si rende disponibile a specifici audit in tema di privacy e sicurezza informatica da parte del Committente.

9.2 L'esperimento di tali audit non deve avere ad oggetto dati di terze parti, informazioni sottoposte ad obblighi di riservatezza degli interessi commerciali.

10. Indagini dell'Autorità e reclami

10.1 Nei limiti della normativa applicabile, LepidaScpA o qualsiasi SubResponsabile informa senza alcun indugio il Committente di qualsiasi

a) richiesta o comunicazione promanante dal Garante per la protezione dei dati personali o da forze dell'ordine;
b) istanza ricevuta da soggetti interessati;

LepidaScpA fornisce, in esecuzione del contratto e, quindi, gratuitamente, tutta la dovuta assistenza al Committente per garantire che la stessa possa rispondere a tali istanze o comunicazioni nei termini temporali previsti dalla normativa e dai regolamentari applicabili.

11. Violazione dei dati personali e obblighi di notifica

11.1 LepidaScpA, in virtù di quanto previsto dall'art. 33 del Regolamento, deve comunicare a mezzo di posta elettronica certificata al Committente nel minor tempo possibile, e comunque non oltre 24 (ventiquattro) ore da quando ne abbia avuto notizia, qualsiasi violazione di sicurezza che abbia comportato accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, ivi incluse quelle che abbiano riguardato i propri sub-Fornitori. Tale comunicazione deve contenere ogni informazione utile alla gestione del *data breach,* oltre a

A. descrivere la natura della violazione dei dati personali;
B. le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
C. i recapiti del DPO nominato o del soggetto competente alla gestione del data breach;
D. la descrizione delle probabili conseguenze della violazione dei dati personali;
E. una descrizione delle misure adottate o che si intende adottare per affrontare la Violazione della sicurezza, compreso, ove opportuno, misure per mitigare i suoi possibili effetti negativi.

11.2 LepidaScpA deve fornire tutto il supporto necessario al Committente ai fini delle indagini e sulle valutazioni in ordine alla violazione di dati, anche al fine di individuare, prevenire e limitare gli effetti negativi della stessa, conformemente ai suoi obblighi ai sensi del presente articolo e, previo accordo con Committente, per svolgere qualsiasi azione che si renda necessaria per porre rimedio alla violazione stessa. LepidaScpA non deve rilasciare, né pubblicare alcun comunicato stampa o relazione riguardante eventuali data breach o violazioni di trattamento senza aver ottenuto il previo consenso scritto del Committente.

12. Responsabilita' e manleve

12.1 LepidaScpA tiene indenne e manleva il Committente da ogni perdita, costo, sanzione, danno e da ogni responsabilità di qualsiasi natura derivante o in connessione con una qualsiasi violazione da parte del Fornitore delle disposizioni contenute nel presente Accordo.

12.2 A fronte della ricezione di un reclamo relativo alle attività oggetto del presente Accordo, LepidaScpA:

12.2.1 avverte, prontamente ed in forma scritta, Committente del Reclamo

12.2.2 non fornisce dettagli al reclamante senza la preventiva interazione con Committente

12.2.3 non transige la controversia senza il previo consenso scritto del Committente;

12.2.4 fornisce al Committente tutta l'assistenza che potrebbe ragionevolmente richiedere nella gestione del reclamo.

Il **Responsabile della protezione dei dati** (**DPO**) di Lepida ScpA ai sensi degli artt. 37 e ss. del GDPR - nominato con Delibera del Consiglio di Amministrazione D0318_51 del 28.03.2018 - è il Direttore Divisione Piattaforme&Software Ing. Kussai Shahin - dpo@lepida.it

Allegato 1

GLOSSARIO

"**Garante per la protezione dei dati personali":** è l'autorità di controllo responsabile per la protezione dei dati personali in Italia;

"**Dati personali ":** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

"**GDPR" o "Regolamento":** si intende il Regolamento UE 2016/679 sulla protezione delle persone fisiche relativamente al trattamento dei dati personali e della loro libera circolazione (General Data Protection Regulation) direttamente applicabile dal 25 maggio 2018;

"**Normativa Applicabile":** si intende l'insieme delle norme rilevanti in materia protezione dei dati personali , incluso il Regolamento Privacy UE 2016/679 (GDPR) ed ogni provvedimento del Garante per la protezione dei dati personali e del WP Art. 29.

"**Appendice Security":** consiste nelle misure di sicurezza che il Titolare determina assicurando un livello minimo di sicurezza, e che possono essere aggiornate ed implementate dal Titolare, di volta in volta, in conformità alle previsioni del presente Accordo;

"**Reclamo":** si intende ogni azione, reclamo, segnalazione presentata nei confronti del Titolare o di un Suo Responsabile del trattamento;

"**Titolare del Trattamento":** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

"**Trattamento":** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

"**Responsabile del trattamento"**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

"**Pseudonimizzazione"**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione

che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile