Science you Trust,
Results that Matter

Allegato Standard Misure Tecniche e Organizzative

Allegato II del DPA | Allegato II delle SCC C2P | Allegato II delle SCC C2C

1. Definizioni

1.1. "Amministratore di Sistema": il soggetto che, in ragione delle proprie competenze tecniche, è incaricato di gestire e mantenere sistemi informatici, infrastrutture di rete o applicazioni che trattano Dati Personali di FIS, ivi incluse le funzioni di gestione degli accessi, backup, monitoraggio, amministrazione di database e manutenzione di sistemi di sicurezza informatica ai sensi e per gli effetti del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e successivo aggiornamento del 25 giugno 2009.
1.2. "Backup": la copia di riserva dei Dati Personali e dei sistemi informatici effettuata a intervalli regolari al fine di garantire il ripristino dei dati in caso di Incidente, guasto tecnico o perdita accidentale.
1.3. "Cifratura": il processo crittografico che rende i Dati Personali incomprensibili a chiunque non sia autorizzato ad accedervi;
1.4. Dato Personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ai sensi dell'art. 4(1) GDPR.
1.5. "DPA": l'Accordo sul Trattamento dei Dati Personali sottoscritto dal Titolare e dal Responsabile.
1.6. "GDPR": il Regolamento (UE) 2016/679 come di volta in volta modificato o integrato.
1.7. "Incidente": la violazione di sicurezza che comporta 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 nell'ambito del presente DPA; ai sensi dell'art. 4(12) GDPR; ivi inclusi gli incidenti che coinvolgono i Sub-Responsabili.
1.8. "MFA" (Autenticazione a più fattori / Multi-Factor Authentication): meccanismo di autenticazione che richiede la verifica dell'identità dell'utente tramite almeno due fattori indipendenti appartenenti a categorie diverse.
1.9. "Parti": il Titolare e il Responsabile congiuntamente; "Parte" indica ciascuno di essi singolarmente.
1.10. "Penetration Test": attività di verifica della sicurezza informatica condotta da soggetti qualificati e indipendenti, volta a identificare vulnerabilità sfruttabili nei sistemi che trattano Dati Personali di FIS, mediante simulazione di attacchi informatici controllati;
1.11. "Pseudonimizzazione": il trattamento dei Dati Personali in modo tale che i dati 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 adeguate;
1.12. "Responsabile" / "Fornitore": la persona fisica o giuridica identificata nel Contratto che, ai sensi dell'art. 4(8) GDPR, tratta Dati Personali per conto

Standard Technical and Organisational Measures Annex

Annex II of the DPA | Annex II of the C2P SCCs | Annex II of the C2C SCCs

1. Definitions

1.1. "Backup": the reserve copy of Personal Data and IT systems made at regular intervals in order to ensure the restoration of data in the event of an Incident, technical failure or accidental loss.
1.2. "Controller" / "FIS": F.I.S. Fabbrica Italiana Sintetici S.p.A., with registered office at Viale Milano 26, 36075 Montecchio Maggiore (VI), Italy.
1.3. "DPA": this Data Processing Agreement concluded between the Controller and the Processor.
1.4. "Encryption": the cryptographic process that renders Personal Data unintelligible to anyone not authorised to access it.
1.5. "GDPR": Regulation (EU) 2016/679 as amended or supplemented from time to time.
1.6. "Incident": a security breach that accidentally or unlawfully results in the destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed under this DPA, within the meaning of Article 4(12) GDPR, including incidents involving Sub-Processors.
1.7. "MFA" (Multi-Factor Authentication): an authentication mechanism that requires verification of the user's identity by means of at least two independent factors belonging to different categories.
1.8. "Parties": the Controller and the Processor collectively; "Party" means either of them individually.
1.9. "Penetration Test": an IT security verification activity conducted by qualified and independent parties, aimed at identifying exploitable vulnerabilities in systems that process FIS Personal Data, through the simulation of controlled cyber-attacks.
1.10. "Personal Data": any information relating to an identified or identifiable natural person within the meaning of Article 4(1) GDPR.
1.11. "Processing": any operation or set of operations performed, whether or not by automated means, on Personal Data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission or dissemination, alignment, restriction, erasure or destruction; pursuant to Article 4(2) GDPR.
1.12. "Processor" / "Supplier": the natural or legal person identified in the Agreement who, pursuant to Article 4(8) GDPR, processes Personal Data on behalf of the Controller in its capacity as data processor.
1.13. "Pseudonymisation": the processing of Personal Data in such a manner that the data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organisational measures.

del Titolare in qualità di responsabile del trattamento.
1.13. "RPO" (Recovery Point Objective): il parametro che definisce la quantità massima di dati che può essere persa in seguito a un Incidente, espressa come intervallo temporale massimo tra l'ultimo Backup valido e il momento dell'Incidente;
1.14. "RTO" (Recovery Time Objective): il parametro che definisce il tempo massimo entro il quale i sistemi e i Dati Personali devono essere ripristinati e resi nuovamente disponibili a seguito di un Incidente;
1.15. "SCC C2P": le Clausole Contrattuali Standard – Modulo Due e adottate con Decisione di esecuzione (UE) 2021/914 della Commissione europea del 4 giugno 2021, nella versione pubblicata all'indirizzo https://fisvi.com/data-protection/ e incorporate nel presente DPA.
1.16. "Sub-Responsabile": qualsiasi persona fisica o giuridica, diversa da un dipendente diretto del Responsabile, alla quale il Responsabile affida il compimento di specifiche attività di Trattamento per conto del Titolare.
1.17. ."Titolare" / "FIS": F.I.S.Fabbrica Italiana Sintetici S.p.A., con sede legale in Viale Milano 26, 36075 Montecchio Maggiore (VI).
1.18. "Trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a 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 o diffusione, il raffronto, la limitazione, la cancellazione o la distruzione; ai sensi dell'art. 4(2) GDPR.
1.19. "Vulnerability Assessment": attività sistematica di identificazione, classificazione e valutazione delle vulnerabilità di sicurezza presenti nei sistemi informatici che trattano Dati Personali di FIS; da effettuarsi almeno trimestralmente con produzione di report documentati.

1.14. "RPO" (Recovery Point Objective): the parameter that defines the maximum amount of data that may be lost following an Incident, expressed as the maximum time interval between the last valid Backup and the moment of the Incident.
1.15. "RTO" (Recovery Time Objective): the parameter that defines the maximum time within which systems and Personal Data must be restored and made available again following an Incident.
1.16. "SCCs C2P": the Standard Contractual Clauses – Module Two adopted by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, in the version published at https://fisvi.com/data-protection/ and incorporated into this DPA.
1.17. "Sub-Processor": any natural or legal person, other than a direct employee of the Processor, to whom the Processor entrusts the carrying out of specific Processing activities on behalf of the Controller.
1.18. "System Administrator": the person who, by virtue of their technical expertise, is entrusted with managing and maintaining IT systems, network infrastructures or applications that process FIS Personal Data, including access management, backup, monitoring, database administration and IT security system maintenance functions pursuant to and for the purposes of the Italian Supervisory Authority's measure of 27 November 2008 and subsequent update of 25 June 2009.
1.19. "Vulnerability Assessment": a systematic activity of identification, classification and assessment of security vulnerabilities present in IT systems that process FIS Personal Data, to be carried out at least quarterly with the production of documented reports.

CIFRATURA E PSEUDONIMIZZAZIONE		**ENCRYPTION AND PSEUDONYMISATION**	
Misura	**Documentazione**	**Measure**	**Documentation**
Protezione fisica e/o Cifratura dati a riposo *AES-256 o equivalente per tutti i supporti contenenti Dati Personali*	Attestazione o certificazione (es. ISO 27001 A.10)	Physical protection and/or Encryption at rest *AES-256 or equivalent for all media containing Personal Data*	Attestation or certification (e.g. ISO 27001 A.10)
Cifratura in transito *TLS 1.2 o superiore per tutte le trasmissioni di Dati Personali su rete pubblica o non trusted*	Test di configurazione SSL/TLS (es. Qualys SSL Labs)	Encryption in transit *TLS 1.2 or higher for all transmissions of Personal Data over public or untrusted networks*	SSL/TLS configuration test (e.g. Qualys SSL Labs)
Cifratura e-mail *S/MIME o PGP per trasmissioni di dati particolari (art. 9 GDPR)*	Dichiarazione del responsabile IT	Email encryption *S/MIME or PGP for transmissions of Special Categories of Personal Data (Art. 9 GDPR)*	Statement from IT manager
Pseudonimizzazione *Pseudonimizzazione applicata ove tecnicamente fattibile e proporzionata alla natura dei dati*	Descrizione della soluzione adottata	Pseudonymisation *Pseudonymisation applied where technically feasible and proportionate to the nature of the data*	Description of the solution adopted

Gestione delle chiavi per servizi cloud. *Chiavi crittografiche gestite separatamente dai dati cifrati; rotazione almeno annuale*	Policy di key management	Key management for cloud services *Cryptographic keys managed separately from encrypted data; rotation at least annually*	Key management policy

CONTROLLO DEGLI ACCESSI		**ACCESS CONTROL**	
Misura	**Documentazione**	**Measure**	**Documentation**
Autenticazione a più fattori (MFA) *MFA obbligatoria per tutti gli accessi remoti e per gli accessi ai sistemi contenenti Dati Personali*	Configurazione sistema / policy	Multi-Factor Authentication (MFA) *MFA mandatory for all remote access and for access to systems containing Personal Data*	System configuration / policy
Principio del minimo privilegio *Accesso ai Dati Personali limitato al personale strettamente necessario (need-to-know); diritti di accesso documentati*	Matrice accessi / IAM system	Least privilege principle *Access to Personal Data limited to strictly necessary personnel (need-to-know); access rights documented*	Access matrix / IAM system
Revisione degli accessi *Revisione periodica dei diritti di accesso almeno semestrale; revoca immediata in caso di cessazione del rapporto*	Report di revisione accessi	Access review *Periodic review of access rights at least every six months; immediate revocation upon termination of employment*	Access review report
Account Amministratori di Sistema *Account con privilegi amministrativi distinti dagli account di uso quotidiano; log di tutte le azioni privilegiate*	Policy account privilegiati	System Administrator accounts *Accounts with administrative privileges separate from everyday-use accounts; log of all privileged actions*	Privileged account policy
Gestione delle credenziali *Password policy: minimo 12 caratteri, complessità, no riuso delle ultime 10 password*	Configurazione del sistema	Credential management *Password policy: minimum 12 characters, complexity requirements, no reuse of last 10 passwords*	System configuration

DISPONIBILITA' E RESILIENZA		**AVAILABILITY AND RESILIENCE**	
Misura	**Documentazione**	**Measure**	**Documentation**
Backup *Backup almeno ogni 2 giorni dei Dati Personali; conservazione per almeno 30 giorni*	Policy di backup	Backup *Backup of Personal Data at least every 2 days; retention for at least 30 days*	Backup policy
Test di ripristino *Verifica periodica dell'integrità e della ripristinabilità dei Backup almeno annuale*	Report test di ripristino	Restoration testing *Periodic verification of the integrity and restorability of Backups at least annually*	Restoration test report
Disaster Recovery *Piano DR documentato con RTO ≤ 24h e RPO ≤ 24h per Dati Personali; test annuale del piano*	Piano DR e report test	Disaster Recovery *Documented DR plan with RTO ≤ 24h and RPO ≤ 24h for Personal Data; annual test of the plan*	DR plan and test report
Alta disponibilità *Ridondanza dei componenti critici (server, rete, storage) per i sistemi che trattano Dati Personali*	Architettura di sistema	High availability *Redundancy of critical components (servers, network, storage) for systems processing Personal Data*	System architecture
Monitoraggio Monitoring *Monitoraggio continuativo della disponibilità dei*	Tool di monitoring	Monitoring *Continuous monitoring of system availability;*	Monitoring tool

sistemi; alert automatici in caso di anomalie		*automatic alerts in the event of anomalies*	

GESTIONE DEGLI INCIDENTI		**INCIDENT MANAGEMENT**	
Misura	**Documentazione**	**Measure**	**Documentation**
Procedura di incident response *Procedura documentata e testata per la gestione degli incidenti di sicurezza; aggiornata almeno annualmente*	Procedura e report test	Incident response procedure *Documented and tested procedure for managing security incidents; updated at least annually*	Procedure and test report
Notifica a FIS *Notifica a FIS nei termini stabiliti dal DPA*	SLA di notifica definito	Notification to FIS *Notification to FIS within the timeframes set out in the DPA*	Defined notification SLA
Log di sicurezza Amministratori di Sistema *Log di accesso e attività in conformità al DPA*	Configurazione SIEM/log	System Administrator security logs *Access and activity logs in accordance with the DPA*	SIEM/log configuration
Analisi post-incidente *Root cause analysis documentata entro 15 giorni dalla chiusura dell'Incidente; condivisione con FIS su richiesta*	Report RCA	Post-incident analysis *Documented root cause analysis within 15 days of Incident closure; shared with FIS upon request*	RCA report
Classificazione degli incidenti *Sistema di classificazione degli incidenti per gravità (critico, alto, medio, basso) con SLA di risposta differenziati*	Policy di classificazione	Incident classification *Incident classification system by severity (critical, high, medium, low) with differentiated response SLAs*	Classification policy

GESTIONE DELLE VULNERABILITA'		**VULNERABILITY MANAGEMENT**	
Misura	**Documentazione**	**Measure**	**Documentation**
Patch management *Patch su servizi esposti online applicate senza ingiustificato ritardo*	Policy e report patch	Patch management *Patches for internet-facing services applied without undue delay*	Policy and patch report
Vulnerability assessment *Scansione di vulnerabilità almeno trimestrale sui sistemi che trattano Dati Personali*	Report scansioni	Vulnerability assessment *Vulnerability scanning at least quarterly on systems processing Personal Data*	Scan reports
Penetration Test *Penetration Test almeno ogni 2 anni sui sistemi che trattano Dati Personali; risultati condivisibili su richiesta*	Report pentest	Penetration Test *Penetration Test at least every 2 years on systems processing Personal Data; results available upon request*	Pentest report
Gestione del software *Inventario aggiornato del software; rimozione del software non più supportato; no software EOL per sistemi con Dati Personali*	Inventario software	Software management *Up-to-date software inventory; removal of unsupported software; no EOL software on systems with Personal Data*	Software inventory
Web application security *Test OWASP Top 10 per applicazioni web che trattano Dati Personali*	Report test OWASP	Web application security *OWASP Top 10 testing for web applications processing Personal Data*	OWASP test report

SICUREZZA DEL PERSONALE		**PERSONNEL SECURITY**	
Misura	**Documentazione**	**Measure**	**Documentation**

Formazione *Formazione sulla protezione dei dati personali almeno annuale per tutto il personale autorizzato al trattamento di Dati Personali;*	Registro formazione	Training *Data protection training at least annually for all personnel authorised to process Personal Data*	Training register
Riservatezza *NDA o clausola di riservatezza specifica per tutto il personale (dipendenti, consulenti, collaboratori) con accesso a Dati Personali*	Copie accordi	Confidentiality *NDA or specific confidentiality clause for all personnel (employees, consultants, contractors) with access to Personal Data*	Copies of agreements
Background check *Verifica dell'idoneità del personale in accesso a Dati Personali, nei limiti consentiti dalla legge applicabile*	Policy HR	Background check *Suitability verification for personnel accessing Personal Data, within the limits permitted by applicable law*	HR policy
Referente privacy *Designazione di un referente per la protezione dei dati, reperibile da FIS per comunicazioni urgenti*	Dati del referente	Privacy contact *Designation of a data protection contact, reachable by FIS for urgent communications*	Contact details
Formazione specifica *Formazione specifica per Amministratori di Sistema che accedono a Dati Personali, con registro delle sessioni*	Registro Amministratori di Sistema	Specific training *Specific training for System Administrators accessing Personal Data, with a register of sessions*	System Administrator register

SICUREZZA FISICA E AMBIENTALE		**PHYSICAL AND ENVIRONMENTAL SECURITY**	
Misura	**Documentazione**	**Measure**	**Documentation**
Accesso fisico ai data center *Accesso fisico ai data center limitato al personale autorizzato; sistema di controllo degli accessi fisici (badge, biometria o equivalente)*	Descrizione sistema	Physical access to data centres *Physical access to data centres limited to authorised personnel; physical access control system (badge, biometrics or equivalent)*	System description
Clean desk e screen lock *Policy di clean desk obbligatoria; screen lock automatico dopo max 5 minuti di inattività*	Policy aziendale	Clean desk and screen lock *Mandatory clean desk policy; automatic screen lock after a maximum of 5 minutes of inactivity*	Company policy
Protezione dispositivi mobili *Cifratura obbligatoria dei dispositivi mobili (laptop, smartphone, tablet) con accesso a Dati Personali; remote wipe attivato*	MDM policy	Mobile device protection *Mandatory encryption of mobile devices (laptops, smartphones, tablets) with access to Personal Data; remote wipe activated*	MDM policy
Smaltimento supporti *Cancellazione sicura (sovrascrittura multi-pass o distruzione fisica certificata) prima dello smaltimento di supporti contenenti Dati Personali*	Certificati di distruzione	Media disposal *Secure erasure (multi-pass overwriting or certified physical destruction) prior to disposal of media containing Personal Data*	Destruction certificates
Protezione ambienti cloud *configurazione sicura (CIS Benchmarks o equivalente); separazione dei Dati Personali da dati di altri clienti*	Report configurazione	Cloud environment protection *Secure configuration (CIS Benchmarks or equivalent); segregation of Personal Data from other customers' data*	Configuration report

CANCELLAZIONE E RESTITUZIONE DEI DATI		DATA DELETION AND RETURN	
Misura	**Documentazione**	**Measure**	**Documentation**
Cancellazione Dati Personali *Cancellazione sicura dei Dati Personali in conformità al DPA*	Procedura di cancellazione e certificato di cancellazione	Personal Data deletion *Secure deletion of Personal Data in accordance with the DPA*	Deletion procedure and deletion certificate
Metodo di cancellazione *Sovrascrittura sicura (NIST 800-88 o equivalente) o distruzione fisica per supporti non riscrivibili*	Documentazione metodo	Deletion method *Secure overwriting (NIST 800-88 or equivalent) or physical destruction for non-rewritable media*	Method documentation
Restituzione dei dati *Su richiesta di FIS, esportazione dei dati in formato interoperabile (CSV, JSON, XML o formato concordato) in conformità al DPA*	Procedura di export	Data return *Upon FIS's request, export of data in an interoperable format (CSV, JSON, XML or agreed format) in accordance with the DPA*	Export procedure