MISURE DI SICUREZZA / SECURITY MEASURES

1. Descrizione delle misure di sicurezza tecniche ed organizzative Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire un livello di sicurezza non inferiore a quello previsto dalle misure tecniche e organizzative di seguito descritte. Quale considerazione generale e preliminare si osservi come non tutte le misure di sicurezza di seguito descritte risultano applicabili e/o implementate su tutti i sistemi e gli applicativi del Responsabile. **2. Amministratori di Sistema** Il Responsabile si impegna a rispettare il Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 (e sue successive modifiche) denominato "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema". **2.1 Designazione** Il Responsabile e gli eventuali Sub-Responsabili si impegnano a redigere una lettera di designazione individuale per ogni amministratore di sistema, successivamente alla valutazione dell'esperienza, della capacità e dell'affidabilità dei soggetti, contenente l'elencazione analitica degli ambiti di operatività. **2.2 Revisione del lavoro degli Amministratori di Sistema** Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere, con cadenza almeno annuale, a un processo di revisione dell'operato degli amministratori di sistema tramite i mezzi che riterranno adeguati. **2.3 Lista degli Amministratori di Sistema** Il Responsabile e gli eventuali Sub-Responsabili si impegnano a produrre, su richiesta del Titolare, una lista del personale designato quale amministratore di sistema recante l'elenco delle funzioni ad esso attribuite. **2.4 Logging** Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare un software di operational intelligence che produca dei log di accesso relativi ai sistemi su cui operano gli amministratori di sistema, aventi caratteristiche di completezza e inalterabilità nonché passibili di verifica di integrità e da conservare per almeno sei mesi.	**1. Description of the organizational and technical security measures** The Data Processor and Sub-processors, if any, undertake to guarantee a level of security that is not inferior to the technical and organisational measures described below. As a general and preliminary consideration, it should be noted that not all the security measures described below are applicable and/or implemented on all the systems and applications of the Data Processor. **2. System Administrators** The Data Processor undertakes to comply with the Provision of the Italian Supervisory Authority of 27 November 2008 (and its subsequent amendments) entitled "Measures and precautions prescribed for data controllers of processing operations carried out by electronic means with regard to the attribution of system administrator functions" **2.1 Designation** The Data Processor and Sub-processors, if any, undertake to draw up an individual letter of appointment for each system administrator, following an assessment of the experience, capacity and reliability of the individuals, containing an analytical list of their areas of operation. **2.2 Review of the work of the System Administrators** The Data Processor and Sub-processors, if any, undertake to carry out, at least once a year, a review process of the work of the system administrators by the means they deem appropriate. **2.3 List of System Administrators** The Data Processor and Sub-processors, if any, undertake to produce, at the Controller's request, a list of the personnel designated as system administrators with a list of the functions assigned to them. **2.4 Logging** The Data Processor and Sub-processors, if any, undertake to implement operational intelligence software that produces access logs relating to the systems on which the system administrators operate, which must be complete and unalterable, as well as subject to integrity checks and to be kept for at least six months.

3. Autenticazione	**3 Authentication**
3.1 Credenziali Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere alla creazione di una password alfanumerica di almeno 8 caratteri in lunghezza, contenente maiuscole/minuscole e caratteri speciali. In alternativa, Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire il possesso di un token o, per trattamenti di particolare rilevanza in termini sia legali che di criticità per il core business aziendale del Titolare, la verifica di caratteristiche biometriche univoche e univocamente digitalizzabili come ad esempio l'impronta digitale. Il Responsabile e gli eventuali Sub-Responsabili si impegnano, eventualmente, su espressa richiesta del Titolare, a procedere alla combinazione di due o più fattori di autenticazione. Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad applicare i criteri summenzionati su tutti i sistemi e applicazioni aziendali.	**3.1 Credentials** The Data Processor and any Sub-processors undertake to create an alphanumeric password at least 8 characters long, containing upper/lower case letters and special characters. Alternatively, the Data Processor and any Sub-processors undertake to ensure the possession of a token or, for processing operations of particular relevance in terms of both legal requirements and criticality for the Data Controller's core business, the verification of unambiguous biometric characteristics that can be uniquely digitised, such as a fingerprint. The Data Processor and any Sub-processors undertake, if necessary, at the express request of the Data Controller, to proceed with the combination of two or more authentication factors. The Data Processor and any Sub-processors undertake to apply the above-mentioned criteria on all the company's systems and applications.
3.3 Credenziali individuali Il Responsabile e gli eventuali Sub-Responsabili si impegnano a non assegnare credenziali condivise ma di assegnare unicamente credenziali individuali, in particolar modo per quanto riguarda le figure dotate di permessi elevati su sistemi e applicazioni.	**3.3 Individual Credentials** The Data Processor and the Sub-processors, if any, undertake not to assign shared credentials, but only to assign individual credentials, especially with regard to persons with high permissions on systems and applications.
3.4 Segnalazione inattività Il Responsabile e gli eventuali Sub-Responsabili si impegnano affinché tutte le credenziali, eccetto quelle utilizzate per soli scopi di gestione tecnica, quali utenze macchina o credenziali di root, vengano segnalate come inattive dopo sei mesi.	**3.4 Reporting inactivity** The Data Processor and any Sub-processors, if any, undertake to ensure that all credentials, except those used for technical management purposes only, such as machine users or root credentials, are reported as inactive after six months.
3.5 Non disclosure Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare e documentare opportune procedure per accedere ai dati in caso di assenza prolungata dell'incaricato che li detiene. Tali procedure non dovrebbero in alcun caso prevedere la disclosure della password dell'incaricato.	**3.5 Non-disclosure** The Data Processor and the Sub-processors, if any, undertake to implement and document appropriate procedures to access the data in the event of the prolonged absence of the person in charge. Such procedures should in no case provide for the disclosure of password of the person in charge.
4. Salvaguardia dati e dispositivi	**4 Data and Device Protection**
4.1 Protezione delle credenziali Il Responsabile e gli eventuali Sub-Responsabili si impegnano a redigere una policy contenente delle chiare istruzioni circa le cautele da adottare per assicurare la segretezza delle credenziali e la diligente custodia dei dispositivi assegnati.	**4.1 Protection of credentials** The Data Processor and the Sub-processors, if any, undertake to draw up a policy containing clear instructions on the precautions to be taken to ensure the secrecy of credentials and the diligent custody of the assigned devices.
4.2 Protezione da danni e furti Il Responsabile e gli eventuali Sub-Responsabili si	**4.2 Protection against damage and theft** The Data Processor and the Sub-processors, if any,

impegnano a redigere una policy contenente delle chiare istruzioni circa le cautele da adottare per assicurare la salvaguardia dei dispositivi assegnati.	undertake to draw up a policy containing clear instructions on the precautions to be taken to ensure the protection of the assigned devices.
4.3 Protezione delle sessioni Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere ad implementare un sistema di lock screen/screensaver con reinserimento delle credenziali ogni qualvolta non vi è fisicamente un incaricato presente a presidiare/utilizzare la postazione di lavoro. Tale lock screen dovrebbe essere impostato affinché si attivi in automatico dopo meno di 5 minuti di inattività.	**4.3 Session protection** The Data Processor and the Sub-processors, if any, undertake to implement a lock screen/screensaver system with reinsertion of credentials whenever there is no person physically present to supervise/use the workstation. This lock screen should be set to activate.
5. Autorizzazione	**5 Authorisation**
5.1 Esistenza profili autorizzativi Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare un sistema centralizzato per la gestione di autenticazione e autorizzazione. Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere ad un censimento dei permessi effettivamente da attribuire, prima di procedere con la loro assegnazione.	**5.1 Existence of authorisation profiles** The Data Processor and the Sub-processors, if any, undertake to implement a centralised system for the management of authentication and authorisation. The Data Processor and the Sub-processors, if any, undertake to conduct a census of the authorisations actually to be granted, before assigning them.
5.2 Minimizzazione dei permessi Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere in via residuale, non assegnando più permessi del dovuto e tenendo a mente i principi del least privilege e del need to know ossia consentendo la visualizzazione dei soli dati necessari a svolgere la funzione lavorativa, con attribuzione dei permessi minimi su sistemi e applicativi.	**5.2 Minimisation of permits** The Data Processor and the Sub-processors, if any, undertake to proceed on a residual basis, not assigning more permits than necessary and bearing in mind the principles of least privilege and need-to-know, i.e. allowing the display of only the data necessary to perform the job function, with minimum permits assigned on systems and applications.
5.3 Revisione profili Il Responsabile e gli eventuali Sub-Responsabili si impegnano a verificare la coerenza e la presenza dei profili autorizzativi almeno annualmente, e di procedere alla verbalizzazione di tale attività.	**5.3 Profile review** The Data Processor and the Sub-processors, if any, undertake to verify the consistency and presence of the authorisation profiles at least annually, and to record this activity.
6. Difesa	**6 Defence**
6.1 Aggiornamenti Il Responsabile e gli eventuali Sub-Responsabili si impegnano a monitorare e gestire in maniera centralizzata e/o automatizzata gli aggiornamenti, o ad adottare idonei mezzi organizzativi in maniera tale da rendere le macchine e le applicazioni costantemente aggiornate tenendo in particolare considerazione gli aggiornamenti di sicurezza.	**6.1 Updates** The Data Processor and the Sub-processors, if any, undertake to monitor and manage updates in a centralised and/or automated manner, or to adopt suitable organisational means in such a way that the machines and applications are constantly updated, with particular regard to security updates.
6.2 Isolamento sistemi non più supportati Il Responsabile e gli eventuali Sub-Responsabili si impegnano a segregare le macchine che per ragioni di	**6.2 Isolation of systems no longer supported** The Data Processor and the Sub-processors, if any, undertake to segregate machines that are still used for

operatività vengono ancora utilizzate nonostante non siano più supportate da aggiornamenti.	operational reasons despite the fact that they are no longer supported by updates.
6.3 Data protection by design	**6.3 Data protection by design**
Il Responsabile e gli eventuali Sub-Responsabili si impegnano a formalizzare o adottare delle linee guida di data protection by design, assicurandosi che i sistemi aziendali sviluppati internamente siano coerenti con esse.	The Data Processor and the Sub-processors, if any, undertake to formalise or adopt data protection by design guidelines, ensuring that the company's internally developed systems are consistent with them.
6.4 Programmi di protezione allo stato dell'arte	**6.4 State-of-the-art protection programmes**
Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare e mantenere aggiornati software di protezione quali antivirus, la cui gestione dovrebbe avvenire in maniera preferibilmente centralizzata, firewall, contenente preferibilmente moduli IDS e IPS, antispam.	The Data Processor and the Sub-processors, if any, undertake to implement and keep up-to-date protection software such as antivirus, the management of which should preferably be centralised, firewalls, preferably containing IDS and IPS modules, and antispam.
7. Disponibilità dei dati	**7 Data availability**
7.1 Backup	**7.1 Backup**
Il Responsabile e gli eventuali Sub-Responsabili si impegnano a implementare un sistema di backup, formalizzando un piano di backup, documentando le tecnologie in atto all'interno di una policy contenente altresì una procedura per eseguire correttamente tale attività.	The Data Processor and the Sub-processors, if any, undertake to implement a backup system, formalising a backup plan, documenting the technologies in place within a policy that also contains a procedure to correctly perform this activity.
7.2 Piani di ripristino	**7.2 Recovery plan**
Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere ad effettuare test di ripristino, verbalizzare i test effettuati e le procedure di ripristino, documentando, inoltre, i tempi necessari per eseguirle.	The Data Processor and the Sub-processors, if any, undertake to perform recovery tests, record the tests performed and the recovery procedures, also documenting the time required to perform them.
8. Protezione dati	**8 Data protection**
8.1 Cifratura e confinamento	**8.1 Encryption and confinement**
Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare di tecniche di cifratura a tutti i livelli: full disk encryption sulle unità di massa, transparent data encryption sui database, file-level encryption per file contenenti credenziali, tramite l'utilizzo di standard crittografici non deprecati.	The Data Processor and the Sub-processors, if any, undertake to implement encryption techniques at all levels: full disk encryption on mass drives, transparent data encryption on databases, file-level encryption for files containing credentials, through the use of non-deprecated cryptographic standards.
8.2 Pseudonimizzazione	**8.2 Pseudonymization**
Il Responsabile e gli eventuali Sub-Responsabili si impegnano a procedere alla pseudonimizzazione dei dati personali eventualmente presenti all'interno dei database.	The Data Processor and the Sub-processors, if any, undertake to pseudonymise any personal data in the databases.
8.3 Cifratura in transito	**8.3 Encryption in transit**
Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare e documentare le tecnologie di cifratura in transito.	The Data Processor and the Sub-processors, if any, undertake to implement and document encryption technologies in transit.

9. Dispositivi rimovibili	**9 Removable devices**
9.1 Dispositivi rimovibili Il Responsabile e gli eventuali Sub-Responsabili si impegnano a regolamentare l'utilizzo dei supporti rimovibili e la loro protezione. **9.2 Sanitizzazione dei dispositivi rimovibili** Il Responsabile e gli eventuali Sub-Responsabili si impegnano a formalizzare opportune procedure per la distruzione, cifratura e/o formattazione dei dispositivi rimovibili e dei dispositivi aziendali in uso.	**9.1 Removable devices** The Data Processor and the Sub-processors, if any, undertake to govern the use of removable media and their protection. **9.2 Sanitisation of removable devices** The Data Processor and the Sub-processors, if any, undertake to formalise appropriate procedures for the destruction, encryption and/or formatting of removable devices and company devices in use.
10. Ruoli di sicurezza Il Responsabile e gli eventuali Sub-Responsabili si impegnano a definire la funzione aziendale che sia responsabile per la cybersecurity, ossia chi possa ricoprirla in azienda con le relative responsabilità. Ciò può comportare di designare un una figura che abbia l'autorità, in azienda, di perimetrare, sotto il piano della sicurezza, informatica e delle informazioni, i processi dell'organizzazione. Tale figura dovrebbe essere reperibile al fine di riscontrare eventuali incidenti di sicurezza e dovrebbe essere nota a tutti i dipendenti.	**10 Security roles** The Data Processor and the Sub-processors, if any, undertake to define the corporate function that is responsible for cybersecurity, i.e. who may hold this position in the company with the corresponding responsibilities. This may entail designating a figure who has the authority, within the company, to perimeter the organisation's processes in terms of cybersecurity and information security. This figure should be available to detect any security incidents and should be known to all employees.
11. Terze parti **11.1 Contratti** Il Responsabile e gli eventuali Sub-Responsabili si impegnano a redigere tutti i contratti rilevanti con gli outsourcer e con i fornitori in maniera tale che includano anche i requisiti di sicurezza pertinenti al servizio o prodotto fornito. **11.2 Audit di secondo livello** Il Responsabile e gli eventuali Sub-Responsabili si impegnano a verificare periodicamente la coerenza con i requisiti di sicurezza contrattualizzati tramite audit di secondo livello opportunamente contrattualizzati e calendarizzati.	**11 Third parties** **11.1 Agreements** The Data Processor and the Sub-processors, if any, undertake to draft all relevant agreements with outsourcers and suppliers in such a way that they also include security requirements relevant to the service or product provided. **11.2 Second level audits** The Data Processor and the Sub-processors, if any, undertake to periodically verify the consistency with the contracted safety requirements by means of appropriately contracted and scheduled second-level audits.
12. Asset Management Il Responsabile e gli eventuali Sub-Responsabili si impegnano a rimuovere asset e credenziali degli impiegati non più in forze all'interno dell'infrastruttura del Responsabile e Sub-Responsabile, o che abbiano cambiato mansione e asset necessari per svolgere la mansione. Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad effettuare una verifica periodica	**12 Asset Management** The Data Processor and the Sub-processors, if any, undertake to remove the assets and credentials of employees who are no longer in the manager's and sub-manager's infrastructure, or who have changed job description and assets required to perform the job. The Data Processor and the Sub-processors, if any, undertake to carry out periodic verification of the actual removal of assets and credentials.

dell'effettiva rimozione di asset e credenziali.	
13. Sicurezza fisica del Centro Elaborazione Dati (CED)	**13 Physical Security of the Data Processing Centre (EDC)**
13.1 Misure di sicurezza fisica Premettendo che tutti i dati e le piattaforme sono hostate su piattaforme cloud o di aziende certificate, il Responsabile e gli eventuali Sub-Responsabili si impegnano a redigere e implementare procedure formali di accesso per consentire l'accesso fisico al CED. I server e le macchine sulle quali sono conservati i dati del Titolare, all'interno del CED, sono ospitati in strutture che richiedono l'accesso con chiave dotata di scheda elettronica, con allarmi collegati ad eventuali SOC o centri di monitoraggio della sicurezza fisica. Le richieste di accesso alle chiavi dotate di schede elettroniche devono essere sottoposte ad un processo formalizzato di approvazione. Le attività non autorizzate e i tentativi di accesso non andati a buon fine vengono registrati dal sistema di controllo accessi e, se del caso, esaminati. Le porte tagliafuoco del CED sono dotate di allarme. Le telecamere a circuito chiuso sono in funzione sia all'interno sia all'esterno del CED. Il posizionamento delle telecamere è stato progettato per coprire aree strategiche che comprendono, tra l'altro, il perimetro, le porte dell'edificio del CED e le aree di ingresso. Il personale addetto alle operazioni di sicurezza in loco gestisce le apparecchiature di monitoraggio, registrazione e controllo delle telecamere a circuito chiuso. L'impianto di CCTV registra 24 ore al giorno, 7 giorni alla settimana. Le registrazioni sono conservate per almeno 7 giorni, in base all'attività.	**13.1 Physical security measures** Assuming that all data and platforms are hosted on cloud or certified company platforms, the Data Processor and the Sub-processors, if any, undertake to draw up and implement formal access procedures to allow physical access to the DPC. The servers and machines on which the Data Controller's data are stored, within the EDC, are hosted in facilities that require access with keys equipped with electronic cards, with alarms connected to any SOCs or physical security monitoring centres. Requests for key card access must undergo a formalised approval process. Unauthorised activities and unsuccessful access attempts are recorded by the access control system and, where appropriate, investigated. The fire doors of the data centre are equipped with alarms. CCTV cameras are in operation both inside and outside the EDC. The positioning of the cameras is designed to cover strategic areas including, among others, the perimeter, the doors of the EDC building and the entrance areas. On-site security personnel operate the CCTV monitoring, recording and control equipment. The CCTV equipment records 24 hours a day, 7 days a week. Recordings are kept for at least 7 days, depending on activity.
13.2 Visitatori Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad autenticare i visitatori prima dell'accesso al CED. Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad accompagnare all'interno della struttura del CED i visitatori e di predisporre un registro di accesso degli stessi. Al fine accedere all'infrastruttura del CED, i visitatori dovranno (i) ottenere in anticipo l'approvazione da parte dei responsabili del CED per le aree interne che desiderano visitare; (ii) accedere tramite identificazione in loco.	**13.2 Visitors** The Data Processor and the Sub-processors, if any, undertake to authenticate visitors before their access to the EDC. The Data Processor and the Sub-processors, if any, undertake to accompany visitors inside the EDC facility and to prepare an access register for them. In order to gain access to the DPC's infrastructure, visitors shall (i) obtain approval in advance from the EDC managers for the internal areas they wish to visit; (ii) gain access through on-site identification.
13.3 Condizioni del CED Il Responsabile e gli eventuali Sub-Responsabili si impegnano a monitorare costantemente le condizioni del CED, considerando le variabili relative, tra le altre, a temperatura, condizione dell'impianto di raffreddamento, polvere, umidità e a verificare	**13.3 EDC conditions** The Data Processor and the Sub-processors, if any, undertake to constantly monitor the conditions of the EDC, taking into account variables relating to, among others, temperature, condition of the cooling system, dust, humidity and to periodically check the functioning

periodicamente il funzionamento dei sensori.	of the sensors.
14. Controllo degli accessi	**14 Access control**
14.1 Credenziali individuali Il Responsabile e gli eventuali Sub-Responsabili si impegnano a creare credenziali individuali per ciascun incaricato e istruire gli stessi incaricati circa la necessità di non condividere le credenziali.	**14.1 Individual credentials** The Data Processor and the Sub-processors, if any, undertake to create individual credentials for each appointee and instruct them not to share credentials.
14.2 Presenza di profili autorizzativi Il Responsabile e gli eventuali Sub-Responsabili si impegnano, nei limiti di quanto consentito dai sistemi, a creare dei profili autorizzativi ai quali assegnare le utenze create.	**14.2 Presence of authorisation profiles** The Data Processor and the Sub-processors, if any, undertake, to the extent permitted by the systems, to create authorisation profiles to which the users created shall be assigned.
14.3 Network access control Il Responsabile e gli eventuali Sub-Responsabili si impegnano a valutare la possibile introduzione di una soluzione per il NAC (Network Access Control) allo scopo di autenticare le macchine sulla rete.	**14.3 Network access control** The Data Processor and the Sub-processors, if any, undertake to evaluate the possible introduction of a NAC (Network Access Control) solution for the purpose of authenticating the machines on the network.
14.4 Separazione VLAN Il Responsabile e gli eventuali Sub-Responsabili si impegnano a prendere in considerazione la possibilità di segmentare la rete in VLAN separate.	**14.4 VLAN separation** The Data Processor and the Sub-processors, if any, undertake to consider segmenting the network into separate VLANs.
14.5 Sessioni concorrenti Il Responsabile e gli eventuali Sub-Responsabili si impegnano a impostare un numero massimo di sessioni concorrenti sui sistemi per lo stesso utente.	**14.5 Competing Sessions** The Data Processor and the Sub-processors, if any, undertake to set a maximum number of concurrent sessions on the systems for the same user.
14.6 Rate limiting Il Responsabile e gli eventuali Sub-Responsabili si impegnano a impostare un numero massimo di tentativi falliti di login prima del blocco dell'account su tutti i sistemi e applicativi aziendali.	**14.6 Rate limiting** The Data Processor and the Sub-processors, if any, undertake to set a maximum number of failed login attempts before account lockout on all corporate systems and applications.
15. Integrità dei sistemi	**15 System integrity**
15.1 SQL Injection Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad attenzionare e implementare processi di sanitizzazione degli input al fine di scongiurare attacchi noti quali SQL Injection.	**15.1 SQL Injection** The Data Processor and the Sub-processors, if any, undertake to implement input sanitisation processes in order to prevent known attacks such as SQL Injection.
15.2 Gestione password e chiavi di cifratura Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare soluzioni per la gestione di password e chiavi di cifratura.	**15.2 Password and encryption key management** The Data Processor and the Sub-processors, if any, undertake to implement solutions for the management of passwords and encryption keys.
15.3 Assenza di possibile disattivazione Il Responsabile e gli eventuali Sub-Responsabili si impegnano a non consentire agli incaricati, non preposti a funzioni di sicurezza, di poter disattivare le misure di protezione sulle loro macchine.	**15.3 No possible deactivation** The Data Processor and the Sub-processors, if any, undertake not to allow persons not entrusted with security functions to deactivate protection measures on their machines.

16. Vulnerability assessment e penetration testing	**16 Vulnerability assessment and penetration testing**
16.1 Periodicità Il Responsabile e gli eventuali Sub-Responsabili si impegnano a condurre sessioni di Vulnerability assessment e penetration testing sui sistemi aziendali con periodicità almeno annuale.	**16.1 Periodicity** The Data Processor and the Sub-processors, if any, undertake to conduct Vulnerability assessment and penetration testing sessions on company systems at least once a year.
16.2 Automatizzazione Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad impiegare dei tool per il Vulnerability Assessment automatizzato, che tuttavia non deve sostituire quello tradizionale.	**16.2 Automation** The Data Processor and the Sub-processors, if any, undertake to use tools for the automated Vulnerability Assessment, which, however, must not replace the traditional one.
17. Gestione degli incidenti e delle violazioni	**17 Incident and breach Management**
17.1 Procedure di incident handling Il Responsabile e gli eventuali Sub-Responsabili si impegnano a introdurre prassi, protocolli e procedure relative all'incident handling e gestire tutti gli eventi di sicurezza e/o gli incidenti di sicurezza tramite una procedura formalizzata con dei ruoli prestabiliti.	**17.1 Incident handling procedure** The Data Processor and the Sub-processors, if any, undertake to introduce practices, protocols and procedures relating to incident handling and manage all security events and/or security incidents by means of a formalised procedure with pre-established roles.
17.2 Formazione del personale Il Responsabile e gli eventuali Sub-Responsabili si impegnano a rendere edotto il personale relativamente alle procedure di incident handling.	**17.2 Staff training** The Data Processor and the Sub-processors, if any, undertake to educate personnel on incident handling procedures.
17.3 Alert Il Responsabile e gli eventuali Sub-Responsabili si impegnano a prendere in considerazione, se ritenuto funzionale e adeguato al rischio, ad adottare un SIEM, o soluzioni alternative che raggiungano lo scopo di segnalare anomalie e/o attacchi in corso.	**17.3 Alert** The Data Processor and the Sub-processors, if any, undertake to consider, if deemed functional and appropriate to the risk, adopting a SIEM, or alternative solutions that achieve the purpose of reporting anomalies and/or attacks in progress.
17.4 Registro degli incidenti Il Responsabile e gli eventuali Sub-Responsabili si impegnano a stilare e mantenere un registro degli incidenti, che contenga almeno le informazioni in merito a scoperta, analisi, contenimento, mitigazione e recupero dai vari incidenti di sicurezza.	**17.4 Incident record** The Data Processor and the Sub-processors, if any, undertake to establish and maintain an incident log, which shall at least contain information on the discovery, analysis, containment, mitigation and recovery from the various security incidents.
17.5 Comunicazione al titolare Il Responsabile e gli eventuali Sub-Responsabili si impegnano a comunicare tempestivamente, nell'arco di 24 ore dalla scoperta, gli incidenti di sicurezza occorsi sulle loro infrastrutture al Titolare.	**17.5 Communications to the Data Controller** The Data Processor and the Sub-processors, if any, undertake to promptly report security incidents occurring on their infrastructure to the Data Controller within 24 hours of their discovery.
18. Business continuity e Disaster Recovery	**18 Business continuity and Disaster Recovery**
18.1 Business continuity Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire la continuità operativa per tutti i servizi offerti al Titolare, tramite, se del caso, la formalizzazione di un Business Continuity Plan.	**18.1 Business continuity** The Data Processor and the Sub-processors, if any, undertake to ensure business continuity for all the services offered to the Data Controller, by formalising a Business Continuity Plan, where appropriate.

18.2 Disaster recovery Il Responsabile e gli eventuali Sub-Responsabili si impegnano a rendere possibile il ripristinare tutti i dati del Titolare in seguito a disastri, tramite, se del caso, la formalizzazione di una strategia per il Disaster Recovery, includendo policy dettagliate per la conservazione sicura delle copie di backup e loro ripristino. **18.3 Cifratura e custodia** Il Responsabile e gli eventuali Sub-Responsabili si impegnano a prevedere la cifratura del backup e di prevedere procedure sicure per la loro custodia.	**18.2 Disaster recovery** The Data Processor and the Sub-processors, if any, undertake to make it possible to restore all the Data Controller's data following disasters, through, if applicable, the formalisation of a Disaster Recovery strategy, including detailed policies for the secure storage of backup copies and their recovery. **18.3 Encryption and safekeeping** The Data Processor and the Sub-processors, if any, undertake to provide for the encryption of backups and to provide for secure procedures for their safekeeping.
19. Formazione Il Responsabile e gli eventuali Sub-Responsabili si impegnano a formalizzare training periodici di security awareness per tutto il personale d'ufficio, al fine di ridurre l'eventualità di intrusioni, riuscita di phishing o infezione da malware.	**19 Training** The Data Processor and the Sub-processors, if any, undertake to formalise periodic security awareness training for all office staff in order to reduce the possibility of intrusion, successful phishing or malware infection.
20. Registrazione delle operazioni Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare un software di operational intelligence che produca log inalterabili, completi e passibili di verifica d'integrità che operi sui sistemi sui quali sono trattati i dati personali riferibili al Titolare.	**20 Recording of operations** The Data Processor and the Sub-processors, if any, undertake to implement operational intelligence software that produces unalterable, complete and integrity-checkable logs operating on the systems on which personal data referable to the Data Controller are processed.
21. Sviluppo software e gestione ambienti **21.1 Linee guida sviluppo** Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad implementare e adottare linee guida di scrittura del codice sicuro. **21.2 Separazione ambienti** Il Responsabile e gli eventuali Sub-Responsabili si impegnano a separare gli ambienti di test, sviluppo e produzione. **21.3 Formalizzazione dei processi di produzione** Il Responsabile e gli eventuali Sub-Responsabili si impegnano a formalizzare le procedure necessarie al passaggio dall'ambiente di test all'ambiente di produzione. **21.4 Testing** Il Responsabile e gli eventuali Sub-Responsabili si impegnano a testare software e sistemi previo inserimento in produzione. **21.5 Patch**	**21 Software Development and Environment Management** **21.1 Development guidelines** The Data Processor and the Sub-processors, if any, undertake to implement and adopt safe code writing guidelines. **21.2 Separation of environments** The Data Processor and the Sub-processors, if any, undertake to separate the test, development and production environments. **21.3 Formalisation of production processes** The Data Processor and the Sub-processors, if any, undertake to formalise the procedures necessary for the transition from the test environment to the production environment. **21.4 Testing** The Data Processor and the Sub-processors, if any, undertake to test software and systems after they have been put into production. **21.5 Patch**

Il Responsabile e gli eventuali Sub-Responsabili si impegnano a effettuare installazione e disinstallazione delle patch tramite prassi note.	The Data Processor and the Sub-processors, if any, undertake to install and uninstall patches through known practices.
21.6 Protezione dei dati di test Il Responsabile e gli eventuali Sub-Responsabili si impegnano a proteggere i dati di test tramite offuscamento o cifratura e di rendere gli stessi utilizzabili sono a personale autorizzato.	**21.6 Testing data protection** The Data Processor and the Sub-processors, if any, undertake to protect the test data by obfuscation or encryption and to make them usable only by authorised personnel.
22. Change management	**22 Change management**
22.1 Formalizzazione del change management Il Responsabile e gli eventuali Sub-Responsabili si impegnano ad effettuare cambiamenti ai sistemi critici tramite prassi note o procedure formalizzate.	**22.1 Formalizing change management** The Data Processor and the Sub-processors, if any, undertake to make changes to critical systems through known practices or formalised procedures.
22.2 Notifica al Titolare Il Responsabile e gli eventuali Sub-Responsabili si impegnano a notificare il Titolare in merito a notevoli cambiamenti relativi alla User Experience.	**22.2 Notification to the Data Controller** The Data Processor and the Sub-processors, if any, undertake to notify the Data Controller of significant changes relating to the User Experience.
23. Rapporti di lavoro	**23 Employment relationships**
23.1 Prima dell'instaurazione del rapporto di lavoro Il Responsabile e gli eventuali Sub-Responsabili si impegnano a prendere in considerazione le responsabilità della sicurezza delle informazioni durante l'assunzione di dipendenti, collaboratori e personale temporaneo (ad esempio attraverso adeguate descrizioni sulle mansioni da svolgere, controlli pre-assunzione) e ad inserirle all'interno dei contratti (ad esempio con termini e condizioni del rapporto di lavoro e sottoscrizione di ulteriori accordi volti a definire ruoli e responsabilità in tema di sicurezza, obblighi di conformità, ecc.).	**23.1 Before the establishment of the employment relationship** The Data Processor and the Sub-processors, if any, undertake to take the responsibilities of information security into account when hiring employees, collaborators and temporary staff (e.g. by means of adequate job descriptions, pre-employment checks) and to include them in the contracts (e.g. by means of terms and conditions of the employment relationship and the signing of additional agreements defining roles and responsibilities with regard to security, compliance obligations, etc.).
23.2 Durante il rapporto di lavoro Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire che i manager si assicurino che i dipendenti e i collaboratori siano consapevoli e motivati a rispettare i loro obblighi per garantire la sicurezza delle informazioni. Il Responsabile e gli eventuali Sub-Responsabili si impegnano altresì a formalizzare un procedimento disciplinare per gestire gli incidenti relativi alla sicurezza delle informazioni presumibilmente causati dai lavoratori.	**23.2 During the employment relationship** The Data Processor and the Sub-processors, if any, undertake to ensure that managers ensure that employees and contractors are aware of and motivated to fulfil their obligations to ensure information security. The Data Processor and the Sub-processors, if any, also undertake to formalise a disciplinary procedure to deal with information security incidents allegedly caused by employees.
23.3 Conclusione o modifiche al rapporto di lavoro Il Responsabile e gli eventuali Sub-Responsabili si impegnano a gestire gli aspetti relativi alla sicurezza al momento dell'uscita di una persona dall'organizzazione, o nelle ipotesi di modifiche significative al ruolo ricoperto, come la restituzione delle informazioni e delle	**23.3 Termination of or changes to the employment relationship** The Data Processor and the Sub-processors, if any, undertake to manage the security aspects when a person leaves the organisation, or in the event of significant changes to the role held, such as the return of

apparecchiature aziendali in possesso del soggetto uscente, l'aggiornamento dei permessi di accesso, nonché il rispetto dei perduranti obblighi relativi alle informazioni riservate ed ai diritti di proprietà intellettuale, ai termini contrattuali, ecc. ed anche ai doveri etici.	information and company equipment in the outgoing person's possession, the updating of access authorisations, as well as compliance with the continuing obligations relating to confidential information and intellectual property rights, contractual terms, etc., and also ethical duties.
24. Conformità	**24 Compliance**
24.1 Conformità ai requisiti legali e contrattuali Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire che l'organizzazione identifichi e documenti i suoi obblighi alle autorità esterne e ad altre terze parti in relazione alla sicurezza delle informazioni, compresa la proprietà intellettuale, la documentazione contabile, le informazioni relative alla privacy/comunque idonee a consentire l'identificazione personale e la crittografia.	**24.1 Compliance with legal and contractual requirements** The Data Processor and the Sub-processors, if any, undertake to ensure that the organisation identifies and documents its obligations to external authorities and other third parties in relation to information security, including intellectual property, accounting records, privacy/personal identification information and encryption.
24.2 Revisione della sicurezza delle informazioni Il Responsabile e gli eventuali Sub-Responsabili si impegnano a garantire che i progetti dell'organizzazione relativamente alla sicurezza delle informazioni siano revisionati (verificati tramite audit) con modalità tali da garantire l'indipendenza della valutazione e rendicontate alla Direzione. Il Responsabile e gli eventuali Sub-Responsabili si impegnano altresì a garantire che i manager revisionino periodicamente la conformità dei dipendenti e dei sistemi alle policy di sicurezza, alle procedure, ecc., e promuovano azioni correttive ove necessario.	**24.2 Information security review** The Data Processor and the Sub-processors, if any, undertake to ensure that the organisation's information security projects are reviewed (audited) in such a way as to guarantee the independence of the assessment and reported to the Management. The Data Processor and the Sub-processors, if any, also undertake to ensure that managers periodically review the compliance of employees and systems with security policies, procedures, etc., and take corrective action where necessary.