Sicurezza IT e Protezione dei dati
Sintesi delle politiche di gestione

Informativa ai sensi del REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 (GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Questo documento descrive inoltre brevemente le politiche messe in atto dalla cooperativa Arcobaleno per garantire la sicurezza delle infrastrutture che ospitano i dati affidatici in gestione.

Arcobaleno assicura una gestione dei sistemi informatici in linea con i requisiti del GDPR.

Fonti di dati personali e tempi di conservazione

Arcobaleno gestisce le infrastrutture sulle quali vengono archiviati dati personali nel contesto dell'erogazione dei suoi servizi informatici.

I dati saranno archiviati su server gestiti direttamente da Arcobaleno (produzione, sviluppo e backup) per tutta la durata del contratto:

- in riferimento al servizio di fileserver: archivio documentale;
- contestualmente alle richieste di assistenza su siti web o servizi: credenziali di accesso e altri dati ivi presenti;
- in riferimento all'hosting: files e database;
- contestualmente alla fornitura di applicativi: files e database.

I dati non verranno trattati da Arcobaleno e saranno conservati solo fino al termine del contratto tra le parti.

I VOSTRI DATI NON VERRANNO MAI SCANSIONATI o ANALIZZATI, se non da *amministratori di sistema* o incaricati per finalità tecniche legate alla sicurezza, o su esplicita richiesta di autorità di pubblica sicurezza.

Alcuni dati saranno archiviati su server di Microsoft per tutta la durata del contratto:

- in riferimento al servizio di posta elettronica e ai servizi office 365.

Finalità del trattamento

La raccolta e il trattamento dei dati personali ha l'esclusiva finalità di gestire gli aspetti amministrativi (fatturazione dei servizi) e tecnici (erogazione dei servizi), nonché l'eventuale registrazione di domini internet per conto dell'intestatario.

Principi

I servizi sono erogati sulla base dei seguenti principi:

- limitazione della finalità e esattezza;
- limitazione della conservazione;
- qualità, integrità e riservatezza;
- responsabilizzazione del personale.

Misure di sicurezza

Tutti i dati sono ospitati su server con tecnologia e configurazioni specifiche per garantire la massima sicurezza.

Si riportano qui solo le misure di sicurezze principali.
I documenti delle policy di sicurezza completi sono disponibili su richiesta esplicita.

Valutazione dei rischi

Il controllo dei rischi viene effettuato regolarmente e vengono successivamente attuate misure migliorative al fine di ridurre le probabilità che un determinato rischio si verifichi. I controlli sono:

- *preventivi*: predisposizione del sistema IT al fine di ridurre i rischi;
- *investigativi*: analisi continua dello stato del sistema IT tramite auditing e analisi forense.

Monitoraggio continuo

- mantenimento del sistema nel giusto punto di equilibrio, in seguito a nuove richieste e/o a nuove tecnologie;
- gestione di modifiche di rilevanza minore del sistema;
- patching, upgrade dei sistemi software e hardware e update delle relazioni con i fornitori.

Gestione degli amministratori di sistema - System Administration (SA)

- Le credenziali SA sono attribuite al solo personale qualificato come "Amministratore di Rete";
- Le credenziali sono archiviate in un DB cifrato;
- Il personale qualificato come "Amministratore di Rete" e "Operatore di Rete" ha una formazione adeguata alla gestione del sistema di sicurezza.

Network Security

- i server sono protetti con sistemi *anti-intrusione* e *firewall*;
- una serie di servizi raggruppati con il termine ArcoNET, garantiscono la possibilità (via web o remote desktop) per utenti esterni, di usufruire di applicazioni Microsoft senza accedere direttamente alle macchine fisiche interne a Base202. L'accesso viene regolato tramite certificati digitali e credenziali, garantendo un adeguato livello di sicurezza;
- per gli utenti che da remoto devono accedere ai servizi interni, è previsto l'utilizzo di VPN;
- dove necessario, i server e gli apparati di rete sono stati dotati del loro sistema di sicurezza al fine di evitare accessi e violazioni degli stessi.

Application Security

Nel caso vengano forniti applicativi sviluppati da Arcobaleno, il software sviluppato viene sottoposto a test di security policy compliance.

Identity, Authentication e Access Management

- tutti i servizi e i pc sono configurati con un sistema di autenticazione personalizzata;
- un sistema SSO (Single Sign On) permette di gestire una sola password tra Windows, Office365 e VLAN;
- i sistemi di autenticazione Microsoft vengono effettuati tramite dominio basato su Active Directory in ambiente Windows s2012 R2;
- i sistemi di autenticazione Unix sono basati su accesso tramite certificato digitale in esclusivo possesso degli amministratori di rete.

Endpoint, Server e Device Security

I pc affidati alla gestione di Arcobaleno sono configurati secondo criteri che mirano ad aumentare al massimo la protezione dei dati ivi trattati.

In particolare vengono configurati un firewall locale, un sistema antivirus distribuito, il blocco automatico dell'accesso in caso di inattività e l'assegnazione degli IP è centralizzata sulla base del Mac Adress.

Nota: Ogni utente deve essere consapevole che il proprio comportamento potrebbe ridurre l'efficacia delle misure di sicurezza, sotto la propria responsabilità:

- usando password elementari o non sicure;
- comunicando a persone non autorizzate le proprie credenziali di accesso ai servizi o alla configurazione dei servizi;
- usando software non sicuro o malconfigurato;
- usando i servizi su computer o dispositivi non protetti da virus e malware;
- ed altre azioni di vario tipo.

Arcobaleno emana periodicamente un aggiornamento delle politiche di protezione dei dati rivolto a tutti gli utenti contenente le buone pratiche per operare in sicurezza.

Crittografia

Laddove necessario o esplicitamente richiesto vengono attivati sistemi di criptaggio.

High Availability, Disaster Recovery e Physical Protection

- sono operative e descritte delle procedure di backup e di disaster recovery;
- sono previsti sistemi ridondanti o in cluster;
- i server di backup sono situati in un'altra sede rispetto al data center.

Soggetti autorizzati all'accesso

Arcobaleno verifica con cura che ogni accesso all'infrastruttura e ai dati da parte di soggetti terzi sia stato autorizzato, e che il soggetto terzo operi nel rispetto del Regolamento (UE) 2016/679.

Trasferimento dei dati personali verso Paesi non appartenenti all'Unione Europea

I dati raccolti ed elaborati non vengono trasferiti presso Società o altre entità al di fuori del territorio comunitario senza che sia stata verificata l'applicazione del presente Regolamento da parte del destinatario.

Tutti i server Arcobaleno sono fisicamente in Italia. Tutti i server di Microsoft sono situati in Europa

Destinatari

I dati identificativi dei clienti potrebbero essere comunicati per finalità amministrative o contrattuali a:

- Microsoft (posta elettronica)
- OVH srl (registrazione domini)
- Aruba srl (registrazione domini)

Diritto all'accesso, rettifica, opposizione e cancellazione

Il cliente può chiedere in qualsiasi momento di:

- accedere ai propri dati;
- avere informazioni sulle finalità del trattamento, sulle categorie di dati trattati, sui dati che sono oggetto di trattamento, sull'origine (per quanto disponibile) dei dati oggetto di trattamento;
- fare rettificare i propri dati (o farne bloccare il trattamento, se del caso) da parte del titolare del trattamento che li stia trattando, se i dati sono inesatti;
- chiedere il blocco, se giustificato, al trattamento dei dati personali;
- fare cancellare i propri dati o farne bloccare il trattamento, se del caso, da parte del titolare del trattamento se questi li sta trattando illegalmente.

Ogni interessato può in qualsiasi momento far valere tali diritti inviando una richiesta scritta (e-mail) a privacy@cooparcobaleno.net.

Diritto alla portabilità dei dati

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano.

Nel caso di caselle di posta elettronica, di contenuti web o altri particolari dati, potrebbe essere chiesto un costo tecnico.

Diritto all'informazione

Arcobaleno si impegna a comunicare tempestivamente agli utenti una eventuale violazione dei dati personali (data breach).

Questa informativa potrebbe essere aggiornata in futuro, qualora le modifiche dovessero essere rilevanti, provvederemo ad una comunicazione diretta all'indirizzo di contatto fornito dal cliente.

Contatti

Arcobaleno cooperativa sociale

Ufficio Tecnico - Arcobaleno Servizi IT

privacy@cooparcobaleno.net

P.Iva 06378620014