1 I EDIZIONE 23-5-2018

BEE COMMUNICATIONS S.C.
Via C. Menotti, 3 - 43125 PARMA (PR)
P. IVA e C.F.: 02223460342
info@beetv.it

BEE communications

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DATI

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Dati identificativi soggetto a cui appartiene il registro:
Denominazione: Bee Communications Soc. Coop.
Indirizzo Sede Legale: Via Menotti, 3 PR
P.IVA/C.F.: 02223460342
PEC: bee@pec.it

Legale Rappresentante:
Luca Laurini - Via Baracca, 32 43036 Fidenza PR
Tel. 0039 347 908 5779

Titolare trattamento dati:
Luca Laurini - Via Baracca, 32 43036 Fidenza PR
Tel. 0039 347 908 5779

Responsabile protezione dati (D.P.O.) nominato il 22/05/2018:
Davide Ferrari - Via Gramsci, 59 42024 Castelnovo di Sotto RE
Tel. 0039 335 610 5278

Tipologia dei dati personali raccolti:
Bee Communications raccoglie i dati personali indispensabili all'assunzione a norma di legge come specificato nelle voci seguenti e forniti direttamente dal candidato dipendente. Non vengono raccolti dati usufruendo di altri canali. Non vengono raccolti dati sensibili (idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (art. 4, lett. d, del Codice della Privacy – Dlgs 196/2003).
Eventuali dati riguardanti lo stato di salute vengono raccolti ed utilizzati per poter usufruire di eventuali agevolazioni fiscali o per ottemperare ad obblighi di legge riguardanti comunque l'assunzione (legge 12 marzo 1999, n. 68)

Finalità del trattamento dati personali e conservazione:
Il D.Lgs. 30/06/2003 n.196 ha la finalità di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. La nostra società si troverà a raccogliere dati personali di ogni aspirante dipendente che verranno utilizzati per la:
1. gestione della sua posizione anche attraverso il sistema informatico della società, l'invio di corrispondenza, ecc.;
2. redazione ed emissione delle buste paga;
3. estrazione di informazioni a carattere statistico;
4. effettuazione di tutti gli adempimenti di legge e di contratto.
Il trattamento dei suoi dati personali avverrà a norma di legge, secondo principi di liceità e correttezza ed in modo da tutelare la sua riservatezza. I dati verranno inseriti nelle scritture e nei registri obbligatori per legge ai fini sopra elencati e verranno trasmessi agli Istituti previdenziali ed assistenziali ed agli Uffici finanziari in ottemperanza a quanto prescritto dalla legge per i datori di lavoro.

Data di creazione 23/05/2018
Date di Aggiornamento ...../...../..... - ...../...../..... -...../...../..... -...../...../..... -

BEE communications

TRATTAMENTI EFFETTUATI IN QUALITA' DI TITOLARE

Modalità acquisizione dati personali e conservazione:
L'azienda Bee Communications s.c. acquisisce i dati personali al fine di espletare tutte le procedure necessarie all'assunzione a norma di legge degli individui candidati. I dati personali sono forniti direttamente dagli aspiranti dipendenti con consegna manuale e relative scansioni, o via posta elettronica non certificata. Nel caso di consegna manuale i documenti di riconoscimento vengono scansionati localmente e localmente vengono conservati nel formato .jpg o .pdf nella memoria del computer di amministrazione (vedi nota 1).
Non vengono conservate copie cartacee dei documenti personali.
Insieme agli altri dati personali comunicati verbalmente vengono redatti e conservati in schede in formato .xlsx memorizzate A) localmente nel computer di amministrazione (vedi nota 1) e B) in backup.
A) Queste schede memorizzate localmente sono files .xlsx con apertura protetta da password.
B) Bee Communications amministra la contabilità mettendo in stretta relazione l'attività dei singoli dipendenti e i conteggi delle fatturazioni verso i clienti che commissionano i servizi. Questo modus operandi è strutturato su operazioni contabili che l'amministratore contabile effettua in remoto con accesso protetto da password sulla piattaforma Microsoft® Office365 (vedi nota 2).

Funzione dell'attività di gestione Risorse Umane:
L'azienda Bee Communications s.c. utilizza l'archivio anagrafico dei dipendenti/soci anche per gestire le comunicazioni (cfr. **Finalità del trattamento dati personali e conservazione, comma 1)** necessarie a:
1 l'espletamento dell'attività e delle mansioni di ciascuno;

2 la verifica delle posizioni rispetto ai corsi di formazione obbligatori e facoltativi - D.Lgs.81/08 (ex D.Lgs.626/94)

Destinatari dei dati a terzi:
L'azienda Bee Communications s.c. comunica i dati personali via email (vedi nota 3) oppure moduli online ai soggetti partner collaboratori per quanto attiene la gestione del personale ed in particolare:
1 alla società Obiettivo Impresa srl per calcolo ed emissione della busta paga (cfr. **Finalità del trattamento dati personali e conservazione, comma 2);**
2 alla società Obiettivo Impresa srl nella persona dell'Avvocato Daria Torelli per lo svolgimento di tutela dei propri dipendenti e del loro lavoro eseguito a favore di committenti che si rendessero morosi (cfr. **Finalità del trattamento dati personali e conservazione, comma 3);**
3 agli enti di previdenza sociale (INPS ENPAL ENPALS) per ottemperare agli obblighi riguardanti le assunzioni in agibilità giornaliere tarmite il modulo automatic messo a disposizione online e protetto da password.

BEE
communications

TRATTAMENTI EFFETTUATI IN QUALITA' DI RESPONSABILE

Base giuridica del trattamento:
L'azienda Bee Communications s.c. al momento dell'assunzione e della contestuale comunicazione dei propri dati personali obbligatori per l'assunzione, presenta al dipendente l'informativa **'ex Art 13 e richiesta consenso ex Art 23 DLGS 30/06/2003 n 196 in materia di protezione dati personali** Aggiornamento Maggio 2018' al fine di renderlo consapevole delle modalità di trattamento dati come da regolamento UE GDPR.

Periodo di conservazione dei dati:
Diritti esercitabili dagli utenti:
Processi decisionali automatizzati:
Autoverifica sicurezza piattaforma: test online di Microsoft effettuato il 16 maggio 2018 e intenzione di adottare il white paper di Microsoft

BEE COMMUNICATIONS S.C.
Via C. Menotti, 3 - 43125 PARMA (PR)
P. IVA e C.F.: 02223460342
info@beetv.it

BEE communications

NOTE:

1 Computer notebook, HewlettPackard 15inch, con funzione di server, ubicato presso l'ufficio della sede legale con sistema operativo Windows 10 protetto da password utente.
2 Microsoft ha progettato Office e Office 365 con criteri di privacy e misure di sicurezza leader di settore per proteggere tutti I dati nel cloud, incluse le categorie di dati personali specificate dal GDPR.

La prevenzione della perdita dei dati in Office e Office 365 è in grado di identificare oltre 80 tipi di dati sensibili comuni, tra cui le informazioni finanziarie, mediche e personali. La prevenzione della perdita dei dati permette inoltre alle aziende di definire come agire in risposta all'identificazione, per proteggere le informazioni riservate e prevenirne la divulgazione accidentale.

La funzionalità Governance avanzata dei dati sfrutta le informazioni approfondite di intelligence ed elaborazione assistita per aiutarti a trovare, classificare, definire e gestire il ciclo di vita dei dati più importanti per la tua azienda, nonché a definire criteri appositi.

La ricerca di Office 365 Advanced eDiscovery ti permette di trovare testo e metadati nel contenuto di tutti gli asset di Office 365, come SharePoint Online, OneDrive for Business, Skype for Business Online ed Exchange Online.

Quando un tecnico di servizio Microsoft ha bisogno di accedere ai tuoi dati, il controllo dell'accesso viene esteso a te in modo che tu possa garantirne l'approvazione finale. Le azioni intraprese sono registrate e rese accessibili a te, in modo che possano essere controllate.

Un altro requisito essenziale del GDPR è la protezione dei dati personali dalle minacce per la sicurezza. Le attuali funzionalità di Office 365 per la protezione dei dati e l'identificazione delle violazioni includono:

Advanced Threat Protection di Exchange Online Protection ti aiuta a proteggere l'e-mail da nuovi e sofisticati attacchi malware in tempo reale. Ti permette inoltre di creare criteri che aiutano gli utenti a prevenire l'accesso ad allegati o siti Web dannosi inviati tramite e-mail.

Threat Intelligence ti aiuta a individuare le minacce avanzate e a proteggerti in modo proattivo in Office 365. Le informazioni approfondite sulle minacce, disponibili grazie alla presenza di Microsoft a livello globale, a Intelligent Security Graph e all'input fornito dai cacciatori di minacce informatiche, ti consentono di ottenere in modo rapido ed efficace avvisi, criteri dinamici e soluzioni per la sicurezza.

Advanced Security Management ti permette di identificare l'utilizzo anomalo e ad alto rischio, segnalandoti le potenziali minacce. Puoi anche configurare criteri di attività per monitorare e affrontare le azioni ad alto rischio.

Infine, i log di controllo di Office 365 ti permettono di monitorare e rilevare le attività di utenti e amministratori tra diversi carichi di lavoro in Office 365, per individuare ed esaminare tempestivamente i problemi di sicurezza e adeguamento.

BEE COMMUNICATIONS S.C.
Via C. Menotti, 3 - 43125 PARMA (PR)
P. IVA e C.F.: 02223460342
info@beetv.it

BEE communications

Microsoft - Protecting personal data
gdpr-compliance/protecting-personal-data-quiz
16/05/2018

Does your organization have sufficient technical measures and processes in place to secure personal and sensitive data? b. Some/in progress

Are your data collection, data processing, and supporting technologies built to include privacy and protection principles? b. Somewhat

How much of your personal and sensitive data is currently encrypted both at rest and in transit? b. Most

I would describe my organization's process for classifying and labeling end user sensitive data as:
c. Manual

Which of the following protection policies do you use to classify and label sensitive data?
b. Rights restrictions d. Restricted access

How much control do you have over access to personal and sensitive data (e.g., physical, remote, etc.)?
a. We protect user and admin credentials d. We use passwords

For which types of data can you apply your control policies?
a. Email/communications d. Documents e. Data warehouse f. HR

If a data breach occurred, how would your organization be able to respond?
a. Process in place to notify data subjects b. Process in place to notify authorities within 72 hours

How often does your organization test the effectiveness of technical measures and processes for ensuring security of data processing? d. Two or three times a year

How much of your data currently resides in the cloud? a. All of it

Your GDPR assessment for protecting personal data is:
You're in the "advanced" stage of protecting personal data
Advanced
75% OF CAPABILITY

BEE communications

Microsoft
Protecting personal data
gdpr-compliance/protecting-personal-data-quiz

Does your organization have sufficient technical measures and processes in place to secure personal and sensitive data? b. Some/in progress

Are your data collection, data processing, and supporting technologies built to include privacy and protection principles? b. Somewhat

How much of your personal and sensitive data is currently encrypted both at rest and in transit?
b. Most

I would describe my organization's process for classifying and labeling end user sensitive data as:
c. Manual

Which of the following protection policies do you use to classify and label sensitive data?
b. Rights restrictions d. Restricted access

How much control do you have over access to personal and sensitive data (e.g., physical, remote, etc.)?
a. We protect user and admin credentials d. We use passwords

For which types of data can you apply your control policies?
a. Email/communications d. Documents e. Data warehouse f. HR

If a data breach occurred, how would your organization be able to respond?
a. Process in place to notify data subjects b. Process in place to notify authorities within 72 hours

How often does your organization test the effectiveness of technical measures and processes for ensuring security of data processing? d. Two or three times a year

How much of your data currently resides in the cloud?
a. All of it

BEE communications

Your GDPR assessment for protecting personal data is:
You're in the "advanced" stage of protecting personal data
Advanced
75% OF CAPABILITY

How strong is your data governance program, including policies, enforcement, and documentation?
b. Somewhat strong

How often do you obtain consent before beginning to use personal data?
a. 100% of the time

Which of the following does your standard company privacy notification include?
a. Data controller contact details
b. Purpose and legal basis of processing
c. Third-party sharing details

If someone contacted you and told you to stop using their personal data, how quickly could you comply?
b. Within a few hours

If someone contacted you and asked you to correct their personal data, how quickly could you comply?
b. Within a few hours

If someone contacted you and asked you to port their data to another organization, how quickly could you comply?
b. Within a few hours

If you were required to conduct a Data Protection Impact Assessment (DPIA) under GDPR, how easy would this be for your organization?
c. Neither easy nor difficult

How much of the flow of personal data into and out of the European Union (EU) do you track and record?
e. None/don't know

How much of the flow of personal data to and from third-party service providers do you track and record?
b. Most

How quickly could you respond to an external GDPR audit request?
c. Within 24 hours

Your GDPR assessment for compliance risk is:
Your GDPR compliance processes could be improved
Moderate risk
50% OF CAPABILITY