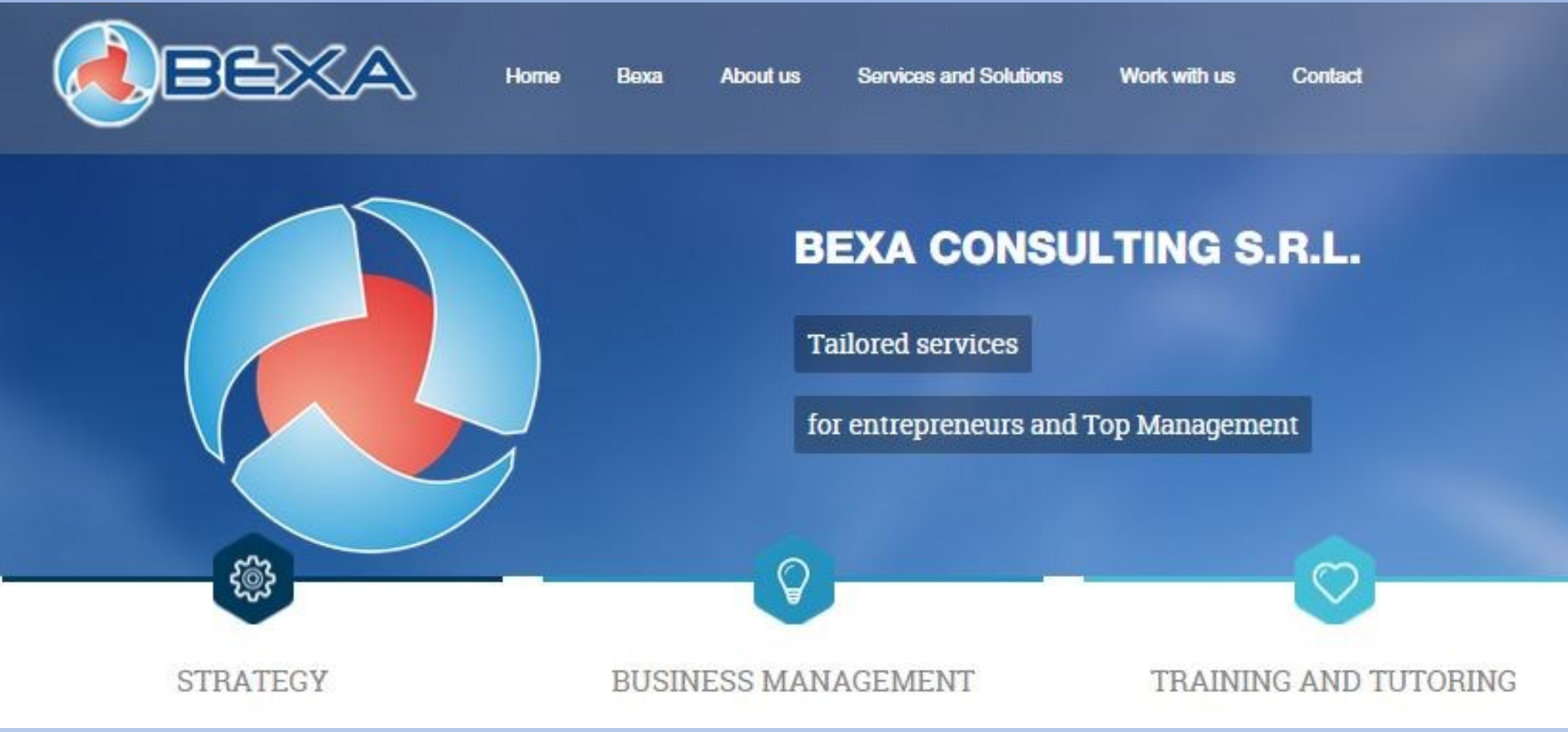


Impatti del GDPR 2016 – Progetto di verifica dell'adeguatezza delle banche dati di un'impresa.
Milano, gennaio 2019

Bexa Consulting srl

Milan - Italy
Via Turati, 29 - 20121
Via Pergolesi, 8 -20124
info@bexa.it

Prima parte - Gli aspetti normativi

1. I riferimenti normativi
2. I fondamenti della legislazione europea sulla privacy e le caratteristiche invariate
3. Principali novità del nuovo GDPR

Riferimenti normativi - 1

- Il nuovo Regolamento UE 2016/679 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati» è definito come **Regolamento Generale sulla Protezione dei Dati**.
- Il nuovo Regolamento è stato approvato il 27 aprile del 2016, è entrato in vigore nel maggio 2016 e sarà applicato a decorrere dal **25 maggio 2018**.
- Contestualmente è stata abrogata la precedente Direttiva 95/46/CE del 1995.
- Tutti i testi originali in italiano dei riferimenti normativi si possono trovare sul sito del Garante per la protezione dei dati personali: http://www.garanteprivacy.it/

Riferimenti normativi - 2

- I fondamenti si trovano nell'articolo 8 della Convenzione Europea dei diritti dell'uomo (approvata nel 1950), dove si afferma che il diritto alla protezione dei dati personali relativamente alla raccolta e all'utilizzo degli stessi è parte del diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza.
- In Italia vige il «Codice privacy», D.L. 196 del 30 giugno 2003, basato principalmente sulla Direttiva 95/46: da maggio 2018 andrà applicato il nuovo GDPR 2016 europeo.

I fondamenti della legislazione europea sulla privacy e le caratteristiche invariate - 1

- La definizione di **dato personale:** qualsiasi informazione riguardante una **persona fisica** identificata o identificabile (**interessato**).
- La definizione di **trattamento**: qualsiasi operazione inerente i momenti di raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento, modifica, uso, estrazione, consultazione, comunicazione, messa a disposizione, raffronto, interconnessione, limitazione, cancellazione e distruzione di dati personali.
- Ogni trattamento deve avere un'idonea base giuridica, di norma basata su un **consenso** espresso dopo aver ricevuto un'apposita **informativa**.
- Gli **interessati sono titolari di diritti** nei confronti delle aziende che trattano i loro dati personali.
- All'interno delle aziende sono identificate le persone (**titolare e responsabili dei trattamenti**), che sono personalmente perseguibili per comportamenti scorretti.

Principali novità del nuovo GDPR- 1

Si tratta principalmente di approfondimenti e/o chiarimenti di punti già presenti nelle normative precedenti:

- il consenso deve essere esplicito anche se non necessariamente per iscritto, per i minori di 16 anni serve il consenso dei genitori;
- vengono specificate le caratteristiche dell'informativa, in termini di contenuti obbligatori (come i tempi di conservazione dei dati e le modalità di contatto dei responsabili aziendali), chiarezza e trasparenza;
- indicazione di un tempo limite di un mese per le aziende per dare risposta agli interessati per tutti i diritti;
- rivisti alcuni diritti (come il diritto di accesso) e introdotti nuovi diritti (diritto all'oblio, alla limitazione del trattamento e alla portabilità dei dati);
- modificate le indicazioni relative alle figure aziendali previste: possibilità di contitolarità del trattamento, di nominare sub-responsabili, obbligo di nominare un responsabile della protezione dati (RDP/DPO).
- nuovi obblighi per i responsabili del trattamento: tenuta di un registro dei trattamenti e adozione di idonee misure tecnico-organizzative per garantire la sicurezza dei trattamenti

Principali novità del nuovo GDPR- 2

La principale novità del nuovo regolamento è sicuramente l'adozione di **un approccio basato sul rischio e di misure di responsabilizzazione (accountability) di titolari e responsabili**:

- titolari e responsabili devono adottare **comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento,** decidendo autonomamente modalità, garanzie e limiti nei trattamenti, rispettando le indicazioni generali del trattamento ed alla luce di alcuni **criteri specifici** indicati nel regolamento**;**
- il principale criterio è la cosiddetta **data protection by default and by design**, cioè la necessità di progettare il trattamento fin dall'inizio per garantire i requisiti indicati dal regolamento e rispettare i diritti degli interessati, alla luce dei rischi specifici del trattamento;
- tale attività richiede un'analisi preventiva e un impegno specifico da parte dei titolari che **devono sostanziarsi in una serie di attività specifiche e dimostrabili**;
- secondo criterio è **il rischio inerente al trattamento,** in termini di impatti negativi sulla libertà e i diritti degli interessati, la cui valutazione spetta al titolare, tramite un apposito processo da effettuare prima del trattamento;
- l'autorità di controllo interverrà quindi solo ex-post e di conseguenza in Italia da maggio 2018 saranno aboliti gli obblighi di notifica preventiva dei trattamenti attualmente esistenti

Seconda parte - Le fasi della verifica

1. Le banche dati, i trattamenti e le informative
2. L'organizzazione e le regole dei processi aziendali
3. I sistemi

Le banche dati, i trattamenti e le informative - 1

- Vanno censite tutte le banche dati contenenti dati personali presenti in azienda, non solo quelle su supporti informatici ma anche gli archivi cartacei.
- Per ogni archivio presente vanno descritti i tipi di dati presenti, con particolare attenzione agli archivi che contengono dati sensibili, cioè dati «che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, e/o trattino dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona» (articolo 9 del regolamento).

Le banche dati, i trattamenti e le informative - 2

- Tutti i dati personali devono essere stati acquisiti in base ad un consenso esplicito e dopo aver consegnato al cliente un'apposita informativa.
- il consenso non va dato necessariamente per iscritto ma il titolare deve essere in grado di dimostrare che è stato dato,
- deve essere, in tutti i casi, libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).
- deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile"
- per i minori di 16 anni va acquisito il consenso dei genitori.

Se non si dispone di consensi adeguati non si possono effettuare trattamenti o detenere dati personali.

Le banche dati, i trattamenti e le informative – 3

- Il nuovo regolamento prevede diverse nuove indicazioni con riguardo all'informativa:
  - deve essere concisa, trasparente e di facile comprensione,
  - deve essere fornita in linea di principio per iscritto,
  - deve essere fornita prima di raccogliere i dati (se raccolti direttamente presso l'interessato),
  - deve informare se sono previsti trattamenti che comportano processi decisionali automatizzati (come la profilazione), in tale caso vanno anche indicate le logiche di tale processo,
  - deve comunicare se i trattamenti previsti comportano il trasferimento dei dati a paesi terzi e attraverso quali strumenti.

L’organizzazione e le regole dei processi aziendali - 1

- I trattamenti effettuati sui dati personali sono anche parte dei processi aziendali.
- I processi aziendali devono prevedere il rispetto dei diritti degli interessati, con particolare riguardo alla cancellazione ed alla trasferibilità dei dati.
- Per ogni archivio/trattamento va verificato chi gestisce i dati personali e che tutti gli addetti abbiano ricevuto le relative lettere di incarico.
- Devono essere stati individuati e nominati i titolari e i responsabili dei trattamenti e, nei casi previsti, il **Data Protection Officer**.
- Va verificato che tutto il personale coinvolto nel trattamento dei dati personali abbia ricevuto le necessarie informazioni sulle normative vigenti.

I sistemi - 1

- Per ogni archivio di dati personali presente in azienda vanno verificate le modalità di conservazione e le misure di sicurezza che impediscono accessi non consentiti.
- In particolare, per i sistemi informatici il nuovo regolamento prescrive l'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento:
  - progettare i sistemi in modo da garantire la necessaria protezione: data protection by design,
  - valutare preventivamente i rischi connessi ai trattamenti, saranno quindi abolite le notifiche preventive previste dall'attuale codice privacy italiano,
  - tenere, nelle aziende con più di 250 dipendenti, un apposito registro dei trattamenti.

I sistemi – 2

- Vanno adottate misure di sicurezza adeguate al rischio.
- Non sono più previsti obblighi generalizzati di adottare specifiche misure minime ma per i sistemi informatici è sempre opportuno verificare:
  - la vulnerabilità del sistema ad accessi non autorizzati,
  - le modalità di accesso, i criteri per cui vengono individuati i dipendenti cui viene concesso l'accesso ai dati, le modalità che permettono di ricostruire chi ha avuto accesso ai dati,
  - le misure di sicurezza che garantiscono che gli accessi siano tracciabili, con particolare riguardo alla gestione delle password,
  - la disponibilità di strumenti che permettano di segnalare un data breach.

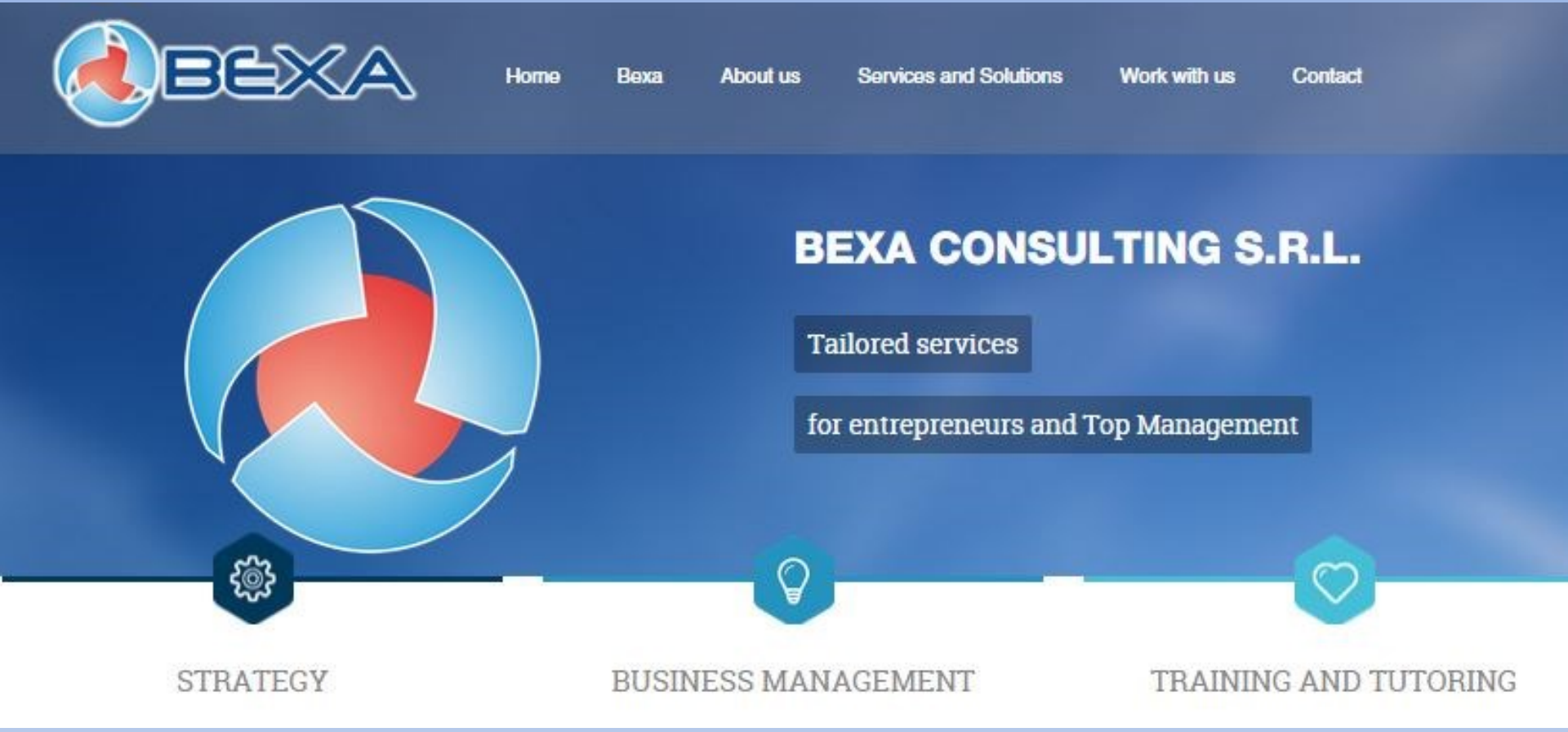
Le attività che BEXA può svolgere- 1

In collaborazione con uno dei principali studi legali di Milano specializzato «storicamente» sulla Data Privacy Bexa propone un approccio su tre passi:

1. Verifica della situazione attuale della vostra azienda in termini di rispetto della Prviacy.
2. Individuazione degli interventi necessari per rispettare il nuovo regolamento.
3. Realizzazione degli interventi, in modo di permettervi di restare concentrati sul vostro business.

Le attività che BEXA può svolgere- 2

1. **Verifica della situazione attuale della vostra azienda in termini di rispetto della Privacy.**
   - Attraverso una semplice check-list viene verificata la situazione della Data Privacy, con un giudizio finale fornito all'azienda
   - La check-list è molto più articolata di quanto offerto oggi gratuitamente sul web
   - E' previsto un supporto telefonico limitato nel caso di dubbi e domande
2. **Individuazione degli interventi necessari per rispettare il nuovo regolamento**
   - Sulla base dei risultati provenienti dal precedente punto viene preparata da Bexa una lista degli interventi necessari a risolvere gli eventuali gap individuati
   - Anche in questo caso è previsto un supporto telefonico più approfondito nel caso di dubbi o domande
3. **Realizzazione degli interventi, in modo di permettervi di restare concentrati sul vostro business**
   - Bexa si occupa di portare a conclusione gli interventi individuati dal precedente step, con un supporto continuativo al cliente
   - Al termine dell'attività viene rilasciato da Bexa un documento in cui si dichiara l'effettuazione di interventi volti ad assicurare il rispetto di quanto richiesto dal regolamento di Data Privacy .



Thank you

Bexa Consulting srl

Milan - Italy
Via Turati, 29 - 20121
Via Pergolesi, 8 -20124
info@bexa.it