Luigi Perrella
CEO & Founder Start Up data Protection

Protezione Dati «INTEGRATA»

Legal – Compliance GDPR
&
Tecnica – Cyber Security

DPO – Data Protection Officer

Certificato UNI 11697/2017

Conosciamo meglio la figura del DPO

1 - CHI E' IL DPO

Il DPO o RDP è una figura introdotta dal GDPR che rappresenta colui che verifica e controlla, in maniera assolutamente indipendente, l'applicazione del regolamento Europeo da parte dell'organizzazione che lo ha designato. E' altresì una figura ufficialmente dichiarata al Garante, attraverso un documento di nomina.

2 – COSA FA IL DPO

Quello che abbiamo detto prima e cioè attività di controllo e verifica, in ambito GDPR, oltre che svolgere un ruolo di consulenza al Titolare e al Responsabile del Trattamento sulle tematiche di protezione dati. Inoltre funge da interfaccia con le autorità preposte.

- E finquì tutto molto semplice e chiaro.

3 CHI PUO' FARE IL DPO ?

«CHIUNQUE»

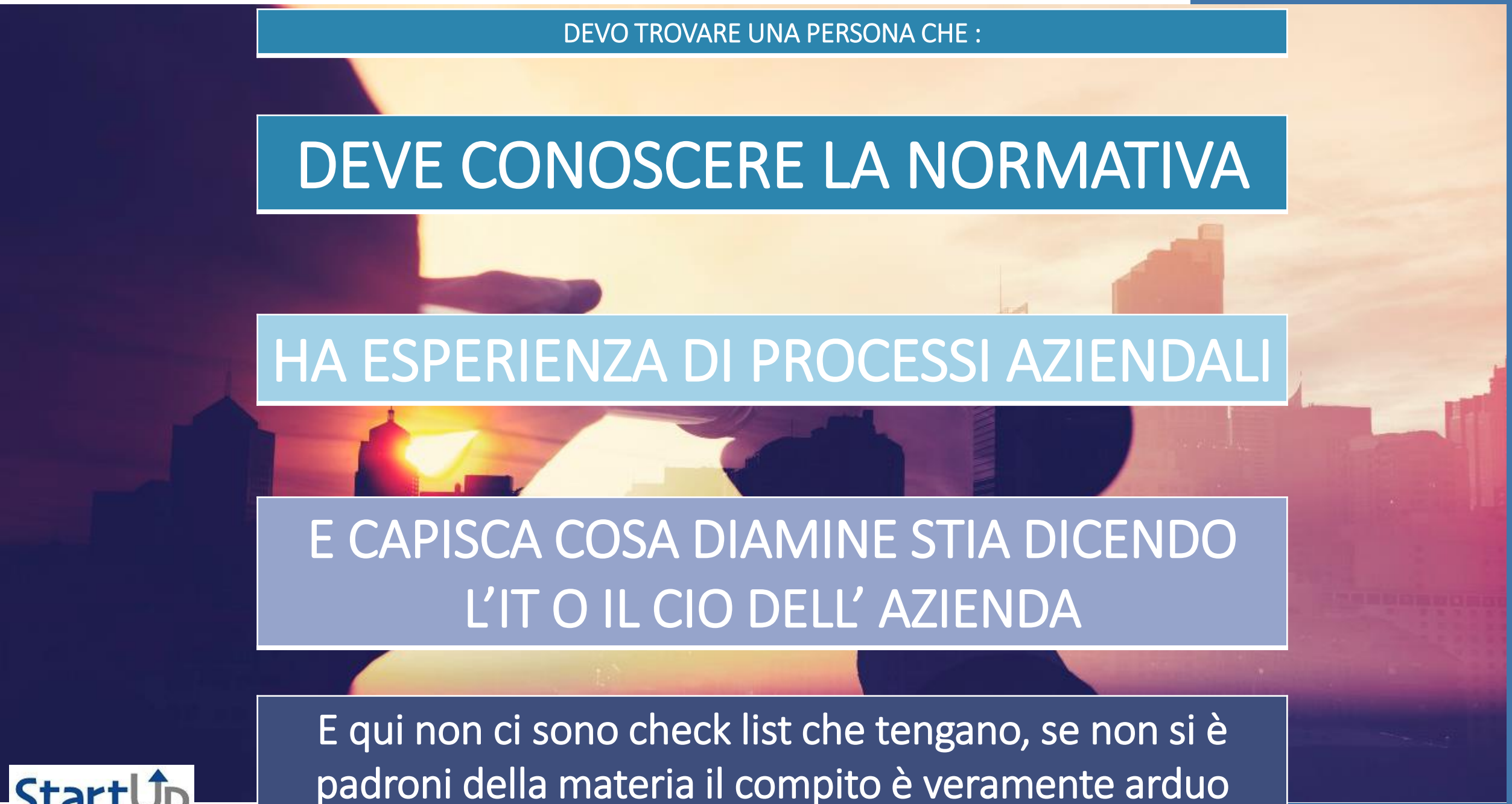
Dal punto di vista tecnico posso chiedere al mio medico o al mio carrozziere di fare il mio DPO, salvo poi incappare in una sanzione per :

«CULPA IN ELIGENDO»

Perchè è vero che posso nominare "chiunque", ma mi devo assicurare che il chiunque sappia svolgere l'incarico e ne abbia le competenze.

E allora questo "CHIUNQUE" chi deve essere ?

StartUp DATA PROTECTION



DEVO TROVARE UNA PERSONA CHE :

DEVE CONOSCERE LA NORMATIVA

HA ESPERIENZA DI PROCESSI AZIENDALI

E CAPISCA COSA DIAMINE STIA DICENDO L'IT O IL CIO DELL' AZIENDA

E qui non ci sono check list che tengano, se non si è padroni della materia il compito è veramente arduo

StartUp DATA PROTECTION

INTERNO O ESTERNO ?

INTERNO

Può essere interno all'azienda ma :

- NON DEVE ESSERE UN APICALE
- NON DEVE RICOPRIRE RUOLI DECISIONALI
- NON PUO' ESSERE L'IT E NE TANTOMENO L'ADS (No conflitti d'interesse)
- DEVE ESSERE INDIPENDENTE
- DEVE ESSERE COMPETENTE NELLA MATERIA (come detto prima)

UNA DECISIONE DIFFICILE DA PRENDERE

ESTERNO

UN LEGALE ?

UN INFORMATICO ?

UN INGEGNERE GESTIONALE ?

UN COMMERCIALISTA ?

«L'importante è che abbia le dovute competenze e bisogna assicurarsene per non incappare nella famosa culpa in eligendo»

StartUp DATA PROTECTION

4 – MA CHI DEVE NOMINARE IL DPO ?

Innanzitutto bisogna partire dal fatto che:

TUTTE LE ORGANIZZAZIONI PUBBLICHE E PRIVATE CHE TRATTANO DATI PERSONALI, DEVONO FARE UN PERCORSO DI ADEGUAMENTO AL GDPR.

OBBLIGATORIAMENTE

«PRINCIPIO DI ACCOUNTABILITY»

- OBBLIGO DI NOMINA in ambito privato

- Monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie di dati particolari e dati su condanne penali e reati
- Società di revisione contabile, Caf e Patronati, utilities (telecomunicazioni),Servizi informatici.

- OPPORTUNITA' DELLA NOMINA

- Non obbligatoria per esempio: in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale o comunque che non effettuano trattamenti su larga scala;
- In ogni caso, resta comunque raccomandata, anche alla luce del principio di accountability che permea il GDPR, la designazione di tale figura.

Quali responsabilità ho come Responsabile Esterno ?

Avete mai verificato se esiste un DPA con i clienti corredato dell'addendum per la nomina a Responsabile esterno ? L'avete mai letta attentamente quella nomina ?

In primo luogo, il Titolare del trattamento deve essere sempre ben consapevole che se affida esternamente un trattamento, deve sempre assegnarlo a soggetti autorevoli e che prestino le idonee garanzie anzidette.
Tale scelta è importantissima al fine di evitare responsabilità in quanto, è ovvio che se si seleziona un soggetto palesemente non idoneo si può profilare la cd. "culpa in eligendo". In seconda battuta, sarà fondamentale nominare il responsabile con atto scritto, che preveda i contenuti prescritti dall'art. 28 del GDPR, soffermandosi in particolare sul tema delle misure di sicurezza e sulle comunicazioni in caso di data breach.
Con l'ordinanza-ingiunzione del 24.03.2022 (doc. web. N. 9767635)

Dall'alto lato, abbiamo visto ora che il Responsabile può ben essere sanzionato per responsabilità diretta e pertanto, dovrà applicare pedissequamente non solo quanto previsto nell'atto di nomina, ma dovrà concentrarsi particolarmente sull'applicazione delle misure di sicurezza e sulle norme previste in tema di protezione di dati personali.

StartUp DATA PROTECTION

STUDIO PROFESSIONALE DEL COMMERCIALISTA

Dati di Bilancio e di Reddito
Dati Patrimoniali e Catastali
Antiriciclaggio
Cassetto Fiscale
Fatturazione Elettronica (valutazione fornitore)
Dati di Pignoramenti e Sequestri Conservativi
Cartelle Esattoriali
Decreti Ingiuntivi
Dati Giudiziali
Dati di Minori e Disabili

Insomma il commercialista, che è prima di tutto un consulente, è la cassaforte dei dati dei propri clienti e degli interessati ad esso legati.

ISP – WISP – SERVIZI INFORMATICI

Dati di traffico internet
Dati di traffico voce
Dati sui server di posta e traffico degli stessi
Dati dei siti web dei clienti
Dati di hosting dei clienti
Dati delle VM e Server di Backup
Dati di e-commerce
Dati di software gestionali
Dati di geolocalizzazione
Dati di videosorveglianza in cloud
Dati di monitoraggio di sicurezza

COSA VOGLIAMO AGGIUNGERE ANCORA ???

E MOLTIPLICATO PER ENNE CLIENTI

IN CASO DI «DATA BREACH»

PERDITA RISERVATEZZA

INTEGRITA’

DISPONIBILITA’DEI DATI (RID)

PERDITA DI OPERATIVITA’

PERDITA ECONOMICA

PERDITA DI REPUTAZIONE

E allora dobbiamo ricorrere ad un sistema di misure tecniche ed organizzative (TOM)

SISTEMI DI SICUREZZA INFORMATICA

StartUp DATA PROTECTION

PROPORZIONATO

SCALABILE

INTEGRATO

GESTITO

StartUp
DATA PROTECTION

4 ELEMENTI BASE

1 – SICUREZZA PERIMETRALE (Firewall)

2 – END POINT E SERVER (ANTIMALWARE-EDR-DLP)

3 – AGGIORNAMENTI E PATCHING

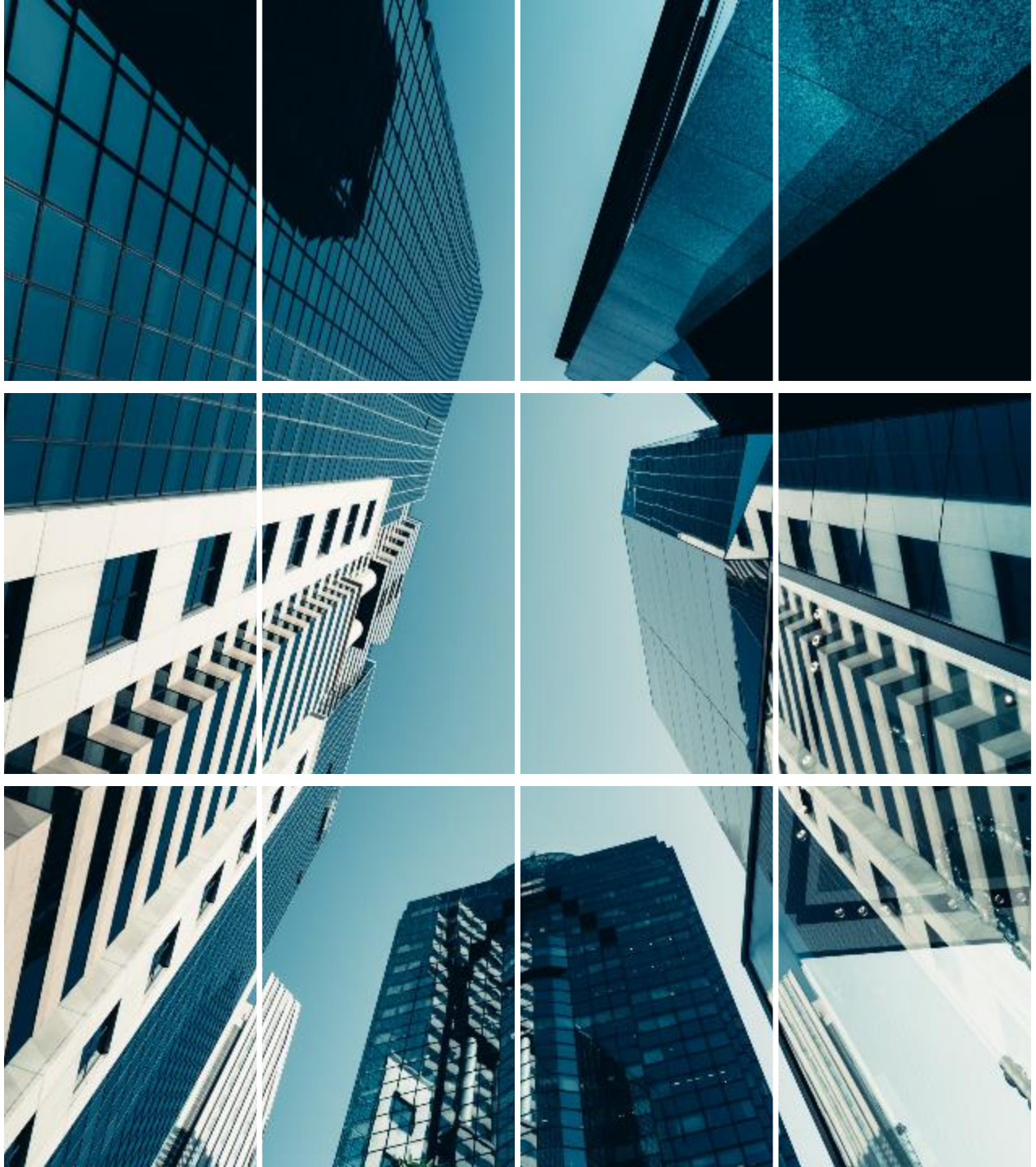
4 – SISTEMA DI BACKUP (LOCALE E CLOUD)

StartUp
DATA PROTECTION

PERCHE’ ABBIAMO DATI CHE:
DOBBIAMO PROTEGGERE PERCHE’ ESISTE UNA NORMATIVA
MA CHE VOGLIAMO PROTEGGERE PERCHE’ SONO IL NOSTRO PATRIMONIO

StartUp
DATA PROTECTION

GESTISCE PATRIMONI DI DATI



StartUp
DATA PROTECTION

Grazie per l'attenzione

luigi.perrella@dpoitalia.eu
+39 393.98.61.526

Siamo a disposizione per qualsiasi supporto,

chiarimento o altro vogliate condividere con NOI.