General Data Protection Regulation (GDPR): Data Protection Services

8 novembre 2017

LEONARDO
SECURITY & INFORMATION SYSTEMS

Indice

- Leonardo - Overview
- Regolamento generale sulla protezione dei dati – GDPR
- Convenzione CONSIP SPC Lotto 2 Sicurezza

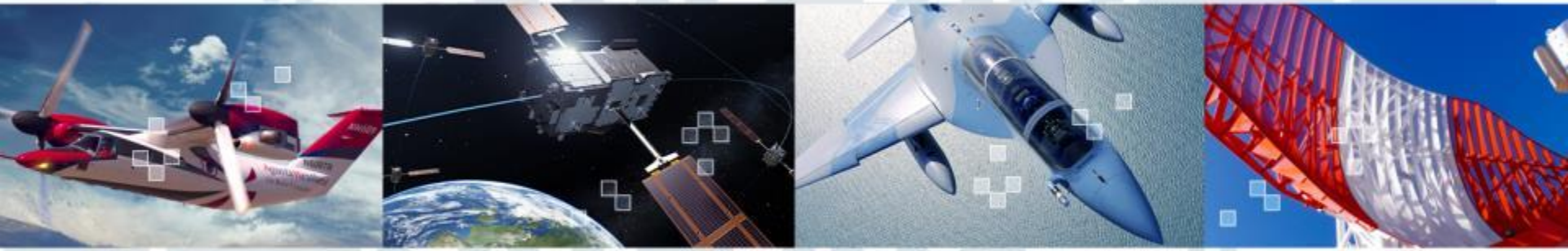
2016: un nuovo capitolo

One Company, più forti insieme

1 gennaio 2016: nasce la **"One Company"**, un'unica società che incorpora per fusione le controllate OTO Melara e WASS e assorbe le attività svolte da AgustaWestland, Alenia Aermacchi, Selex ES. L'azienda mantiene anche le funzioni di Capo Gruppo e *Corporate Centre* per le società **DRS Technologies, MBDA, Telespazio, Thales Alenia Space** e **ATR.**

Finmeccanica rinasce in Leonardo

28 aprile 2016: Finmeccanica assume un nuovo nome, **Leonardo,** ispirato a Leonardo da Vinci, simbolo universalmente riconosciuto di **creatività** e **innovazione**. **Leonardo** rappresenta il ponte ideale tra la storia da cui veniamo e il nostro futuro.



Le nostre attività

Leonardo è un'azienda globale ad alta tecnologia e uno dei protagonisti nel mercato mondiale dell'**Aerospazio, Difesa e Sicurezza.**

DIVISIONI

- **Elicotteri**
- **Velivoli**
- **Aerostrutture**
- **Sistemi Avionici e Spaziali**
- **Elettronica per la Difesa Terrestre e Navale**
- **Sistemi di Difesa**
- **Sistemi per la Sicurezza e le Informazioni**

CONTROLLATE E JOINT VENTURE

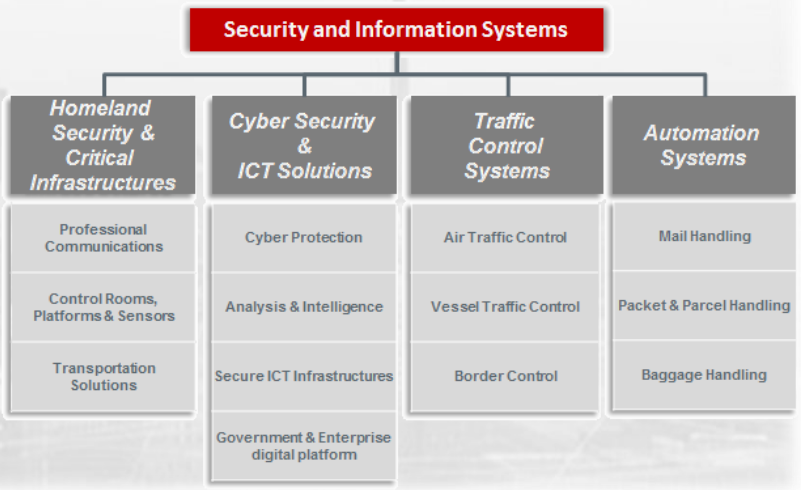
- **DRS Technologies** (100% Leonardo)
- **Telespazio** (67% Leonardo e 33% Thales)
- **Thales Alenia Space** (67% Thales e 33% Leonardo)
- **MBDA** (37,5% BAE Systems, 37,5% Airbus Group, 25% Leonardo)
- **ATR** (50% Leonardo e 50% Airbus Group)

Divisione Sistemi per la Sicurezza e le Informazioni

L'Organizzazione

Una Divisione, 4 Linee di Business, organizzate in Business Area:

- **Homeland Security,** fornisce soluzioni di sicurezza che contribuiscono ad accrescere la situational awareness al fine di proteggere zone a rischio, aree urbane, infrastrutture critiche, siti sensibili e grandi eventi
- **Cyber Security & ICT Solutions,** offre soluzioni digitali secure-by-design, piattaforme di intelligence e servizi gestiti in ambito ICT e Cyber security per abilitare la trasformazione digitale dei Clienti
- **Traffic Control Systems** supporta, attraverso l'utilizzo di tecnologie e soluzioni innovative, la circolazione sicura, veloce ed efficiente del traffico aereo e marittimo e il miglioramento dei livelli di sicurezza dei passeggeri
- **Automation Systems,** realizza soluzioni integrate multi-funzionali per lo smistamento e la tracciatura di pacchi, pacchetti, lettere e bagagli, basate su tecnologie proprietarie all'avanguardia e collaudate sul mercato



Organico Divisione SSI **3.070**

KEY FIGURES 2016

Risultati finanziari di Gruppo – anno 2016 (in €mld.)

RICAVI

12,0

- 46% ELETTRONICA, DIFESA E SISTEMI DI SICUREZZA
- 30% ELICOTTERI
- 26% AERONAUTICA
- 3% ALTRE ATTIVITÀ
- -5% ELISIONI

PORTAFOGLIO ORDINI

34,8

- 38% AERONAUTICA
- 34% ELETTRONICA, DIFESA E SISTEMI DI SICUREZZA
- 31% ELICOTTERI
- 0% ALTRE ATTIVITÀ
- -3% ELISIONI

ORDINI

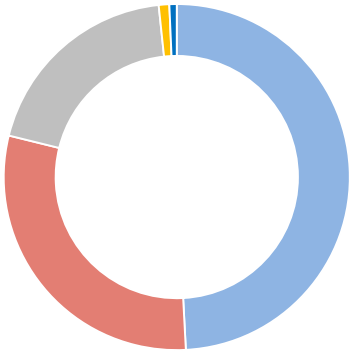
20,0

- 51% AERONAUTICA
- 34% ELETTRONICA, DIFESA E SISTEMI DI SICUREZZA
- 19% ELICOTTERI
- 0% ALTRE ATTIVITÀ
- -4% ELISIONI

RISULTATI 2016 in €mln.

Ricavi	12.002
Ordini	19.951
Portafoglio Ordini	34.798
Ricerca e Sviluppo	1.373
Organico	45.631

COMPOSIZIONE DELL'AZIONARIATO



- 50,4% INVESTITORI ISTITUZIONALI
- 30,2% MINISTERO DELL'ECONOMIA E DELLE FINANZE
- 17,7% INVESTITORI INDIVIDUALI (SOLO ITALIA)
- 1 % ALTRI INVESTITORI ISTITUZIONALI
- 0,7% AZIONI PROPRIE

Indice

Regolamento generale sulla protezione dei dati - GDPR

- Concetti chiave
- Campo di applicazione del GDPR
- Sistema di conformità e principio di “Accountability”
- Trasparenza
- Diritti degli interessati
- Data security
- Data Breach
- Ruoli e responsabilità
- Sistema documentale
- Garanzie per i flussi extra UE
- Privacy by design and by default
- Conformità al GDPR: altri servizi
- Sanzioni di rilevante entità in caso di violazione

Convenzione CONSIP SPC Lotto 2 Sicurezza

- La proposta di Leonardo per supportare gli Enti Sanitari sul nuovo GDPR

Regolamento generale sulla protezione dei dati - GDPR

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

GDPR
EU General Data Protection Regulation

Pubblicato sulla Gazzetta ufficiale dell'Unione europea il 4 maggio 2016.

- **È in vigore dal 24 maggio 2016**
- **Si applica a decorrere dal 25 maggio 2018**
- **Abroga la direttiva 95/46/CE a decorrere dal 25 maggio 2018**

Introduce nuovi diritti, principi, obblighi, adempimenti e regole

Il regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri (non necessita di essere recepito dall'ordinamento nazionale mediante altra legge o norma).

Concetti chiave - protezione e libera circolazione

Protezione e libera circolazione dei dati

Non si parla più solo di protezione dei dati personali ma anche di libera circolazione dei dati.

Concetti chiave - il bene da proteggere: i dati personali

DATI PERSONALI

Qualsiasi informazione relativa a persona fisica (interessato)

Identificata o Identificabile

Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

DATI RELATIVI ALLA SALUTE

I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

DATI BIOMETRICI

DATI GENETICI

ALTRI DATI PERSONALI…

Concetti chiave - trattamento

Qualsiasi operazione o insieme di operazioni applicate ai dati personali

Trattamento

qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali.

Sono operazioni di trattamento:

- la raccolta
- la registrazione
- l'organizzazione
- **la strutturazione**
- la conservazione
- **l'adattamento o** la modifica
- l'estrazione
- la consultazione
- l'uso
- la comunicazione mediante trasmissione
- diffusione **o qualsiasi altra forma di messa a disposizione**
- il raffronto o l'interconnessione
- **la limitazione**
- la cancellazione o la distruzione.

Campo di applicazione del GDPR

Estensione del campo di applicazione: impatto internazionale della normativa

Ambito di applicazione materiale. Il presente regolamento si applica:

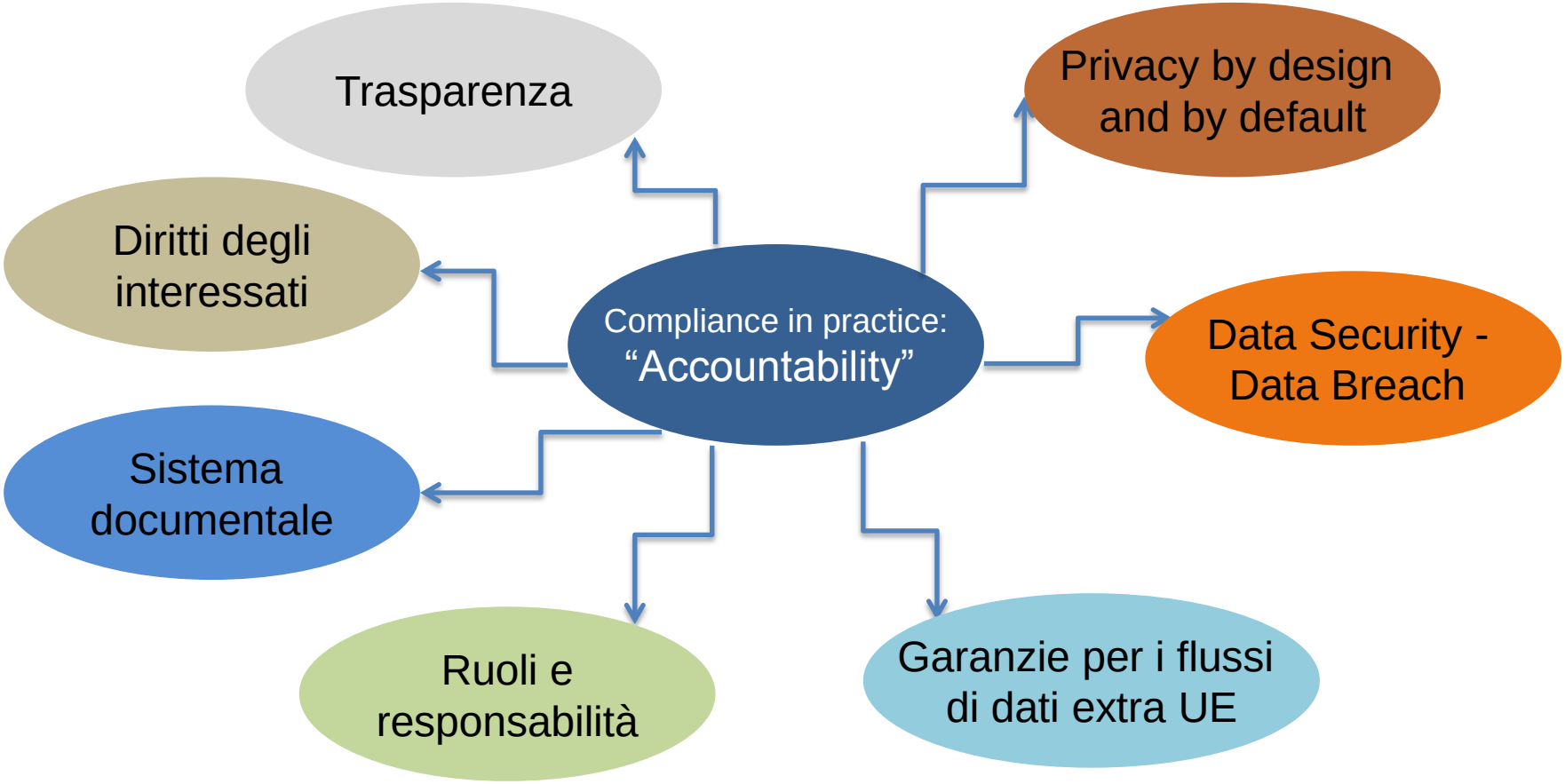
- al trattamento interamente o parzialmente automatizzato di dati personali e
- al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Ambito di applicazione territoriale. Il regolamento in merito alla territorialità introduce un'importante **novità**. **Chi fornirà un servizio in Italia e tratterà dati personali, anche se ha la sede altrove, dovrà sottostare alla normativa europea valida in tutti gli Stati membri**.

Così il regolamento si applica al trattamento dei dati personali:

- effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.
- di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione**, quando le attività di trattamento riguardano ad es. l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione.**

Sistema di conformità e principio di “Accountability”



“Accountability”

«Responsabilizzazione» del titolare nell’applicazione degli adempimenti»

Il titolare del trattamento **deve essere in grado di comprovare, di dimostrare** (innalzamento del livello di responsabilizzazione) l’applicazione dei principi del trattamento, il rispetto delle regole e di avere ottemperato a tutti gli adempimenti prescritti.

A dimostrazione della conformità del titolare al GDPR è possibile far ricorso a specifici strumenti quali l’adesione ai meccanismi di certificazione e/o ai codici di condotta.

Trasparenza

Fornire informazioni chiare ed esaurienti per un trattamento corretto e trasparente.

PRESCRIZIONE

Nel GDPR è prescritto per il titolare del trattamento di assicurare un trattamento corretto e trasparente a tutela degli interessati. Ad esempio, agli art.13 e 14 si prescrive di **fornire agli interessati informazion**i, ad esempio:

- sull'identità e sui dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante e del DPO
- sul trattamento e sulle comunicazioni previste
- sull'intenzione del titolare di trasferire dati personali a un destinatario in un paese terzo
- sul periodo di conservazione dei dati personali
- sul diritto di proporre reclamo a un'autorità di controllo (Garante Privacy).

Inoltre, il Titolare deve rispettare e garantire le condizioni prescritte nel GDPR sulla **prestazione del consenso** al trattamento, qualora sia previsto.

DATA PROTECTION SERVICES

Per rispondere agli obblighi relativi all'informativa sul trattamento e alla prestazione del consenso, ove previsto, **Leonardo propone servizi di**:

- **Redazione e rilascio di Informative in conformità al GDPR**
- **Supporto ai fini degli adempimenti sul consenso**

Diritti degli interessati

Garantire l'accesso ai dati e gli altri diritti degli interessati.

PRESCRIZIONE

Nel GDPR sono individuati importanti diritti per l'interessato. Ad esempio, dagli artt. dal 15 al 20 si descrive che **l'interessato ha diritto** di ottenere da parte del Titolare, ad esempio:

- l'accesso ai dati personali
- una copia dei dati
- la rettifica dei dati
- **NEW la cancellazione («diritto all'oblio»)**
- la limitazione del trattamento
- **NEW la portabilità dei dati**

Inoltre, l'interessato ha diritto di opporsi (art.21) in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano.

DATA PROTECTION SERVICES

Per rispondere a tale obbligo di garanzia dei diritti degli interessati **Leonardo propone servizi finalizzati alla**

- **Gestione dei diritti degli interessati**
- **Predisposizione della modulistica**

Data security

Garantire un livello di sicurezza adeguato al rischio e notifiche di Data Breach.

PRESCRIZIONE

Nel GDPR Il titolare del trattamento e il responsabile del trattamento al fine di garantire la **sicurezza dei dati** trattati (art.32) devono:

- mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (non si prevedono misure minime di sicurezza come nel Codice Privacy).
- valutare che sia raggiunto un adeguato livello di sicurezza
- istruire chiunque tratta i dati sotto la propria autorità (ossia i soggetti che nel Codice Privacy sono gli incaricati del trattamento).

DATA PROTECTION SERVICES

Per rispondere a tale obbligo di sicurezza dei dati personali **Leonardo propone servizi di:**

- **Analisi e gestione del rischio**
- **Security/Cyber Security Assessment**
- **Vulnerability Assessment**
- **Piano degli Interventi**
- **Redazione delle Istruzioni**

Data Breach

Effettuare le notifiche di Data Breach in caso di violazione dei dati.

PRESCRIZIONE

Il GDPR introduce l'**obbligo per il titolare di avvertire l'autorità di controllo** e, qualora vi sia il sospetto che possa averne un danno**,** anche l'interessato **della violazione dei dati personali.**

Il titolare del trattamento deve:

- **notificare la violazione all'autorità di controllo** competente senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**.
- Trasmettere la notifica con le necessarie informazioni indicate nel regolamento.
- **documentare qualsiasi violazione** dei dati e i provvedimenti adottati per porvi rimedio.

Notificazione all'interessato. Il titolare del trattamento, al verificarsi di specifiche condizioni, comunica la violazione all'interessato senza ingiustificato ritardo.

DATA PROTECTION SERVICES

Per rispondere a tale obbligo di notificazione di Data Breach **Leonardo propone servizi di:**

- **NEW Gestione dei Data Breach (procedure, responsabilità, ecc.)**
- **Supporto alla predisposizione di Notificazioni di Data Breach e della documentazione**

Ruoli e responsabilità

Individuazione dei ruoli e delle responsabilità in ambito Data Protection.

PRESCRIZIONE

Secondo Il GDPR devono essere individuati i **ruoli e** le **responsabilità** di tutte le figure coinvolte in ambito Data Protection. Oltre al Titolare del trattamento (Controller) devono essere identificati necessariamente o, ove applicabile i seguenti ruoli:

- **NEW Contitolari del trattamento**
- Responsabile del trattamento (Processor)
- **NEW Rappresentante del titolare o del responsabile** (qualora il trattamento sia effettuato da un soggetto stabilito fuori UE).
- Persone autorizzate al trattamento (i soggetti definiti incaricati dal Codice Privacy)
- **NEW Responsabile della protezione dei dati (Data Protection Officer)** - da non confondere con il responsabile del trattamento.

DATA PROTECTION SERVICES

Per rispondere a tale obbligo di definizione di ruoli e responsabilità in ambito Data Protection, **Leonardo propone servizi finalizzati alla:**

- **Definizione del modello organizzativo di Data Protection**
- **NEW Consulenza tecnica per la definizione dell'incarico e dei compiti del DPO**

Sistema documentale

Obbligo di redazione ed aggiornamento di specifici documenti

PRESCRIZIONE

Il GDPR descrive degli **obblighi di tenuta ed aggiornamento di specifici documenti**. Ad esempio, in particolare:

- Il **registro dei trattamenti** – E' una sorta di DPS e dovrà contenere specifiche informazioni e sono tenuti in forma scritta, anche in formato elettronico (art.30)
- Un documento contenente la **Valutazione dell'impatto dei trattamenti** – da effettuare preventivamente al trattamento
- La richiesta di **consultazione preventiva** all'autorità di controllo sulla base dell'esito «negativo» della Valutazione .

DATA PROTECTION SERVICES

Per rispondere a tale obbligo di definizione di un sistema documentale in conformità al GDPR, **Leonardo propone servizi di:**

- **Censimento dei trattamenti Redazione dei registri, dei documenti, della modulistica ed Aggiornamento periodico**
- **NEW Data protection impact assessment (Analisi dello scenario, valutazione dei rischi e riesame)**

Garanzie per i flussi extra UE

Adeguate garanzie per il trasferimento di dati verso paesi terzi

PRESCRIZIONE

Il GDPR permette che ci possano essere **trasferimenti di dati personali verso un paese terzo** o un'organizzazione internazionale fatto salvo il rispetto di specifiche garanzie, tra cui ad esempio:

- Atti, accordi vincolanti tra PA
- clausole contrattuali standard
- norme vincolanti d'impresa (es. regolamento aziendale vincolante)
- clausole tipo di protezione dei dati adottate da un'autorità di controllo
- codici di deontologia approvati
- meccanismi basati su certificazioni approvate.

ATTENZIONE. Le autorizzazioni al trasferimento rilasciate da uno Stato membro o dall'autorità di controllo ai sensi della direttiva 95/46/CE restano valide fino a quando non vengono modificate, sostituite o abrogate.

DATA PROTECTION SERVICES

Per rispondere a tale obbligo di adeguate garanzie per il trasferimento dei dati verso Paesi terzi, **Leonardo propone servizi di:**

- **NEW Supporto alla redazione degli atti, delle clausole**
- **Consulenza legale-normativa**

Privacy by design and by default

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

PRESCRIZIONE

Il GDPR introduce l'obbligo per tutti di progettare nuovi beni e servizi tenendo sempre a mente le prerogative della minimizzazione del trattamento dei dati (art.26). Per ciò il titolare del trattamento deve:

- **mettere in atto misure tecniche e organizzative adeguate** volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

DATA PROTECTION SERVICES

Per rispondere a tale obbligo di garanzia dei diritti degli interessati **Leonardo propone servizi finalizzati alla**

- **Analisi dei processi**
- **NEW Stesura di procedure ad hoc**

Conformità al GDPR: altri servizi

Attivazione di altri servizi in ottica “Accountability”

PRESCRIZIONE

Tutti i soggetti citati nel GDPR devono rispettare e realizzare gli adempimenti e gli obblighi prescritti.

DATA PROTECTION SERVICES

Per rispondere alla normativa del regolamento, **Leonardo propone altri servizi finalizzati alla:**

- **Sensibilizzazione e formazione di tutti i soggetti coinvolti**
- **Auditing - Verifica e monitoraggio Risoluzione di casi pratici**
- **NEW Supporto ad un sistema di gestione di Data Protection**

Sanzioni di rilevante entità in caso di violazione

Il GDPR introduce un nuovo meccanismo sanzionatori senza precedenti

Sanzioni amministrative pecuniarie fino a 20 milioni di euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Ogni autorità di controllo provvede affinché le **sanzioni** amministrative pecuniarie inflitte in relazione alle violazioni del regolamento siano in ogni singolo caso **effettive, proporzionate e dissuasive.**

Convenzione CONSIP SPC Lotto 2 Sicurezza

La proposta di Leonardo per supportare gli Enti Sanitari sul nuovo GDPR

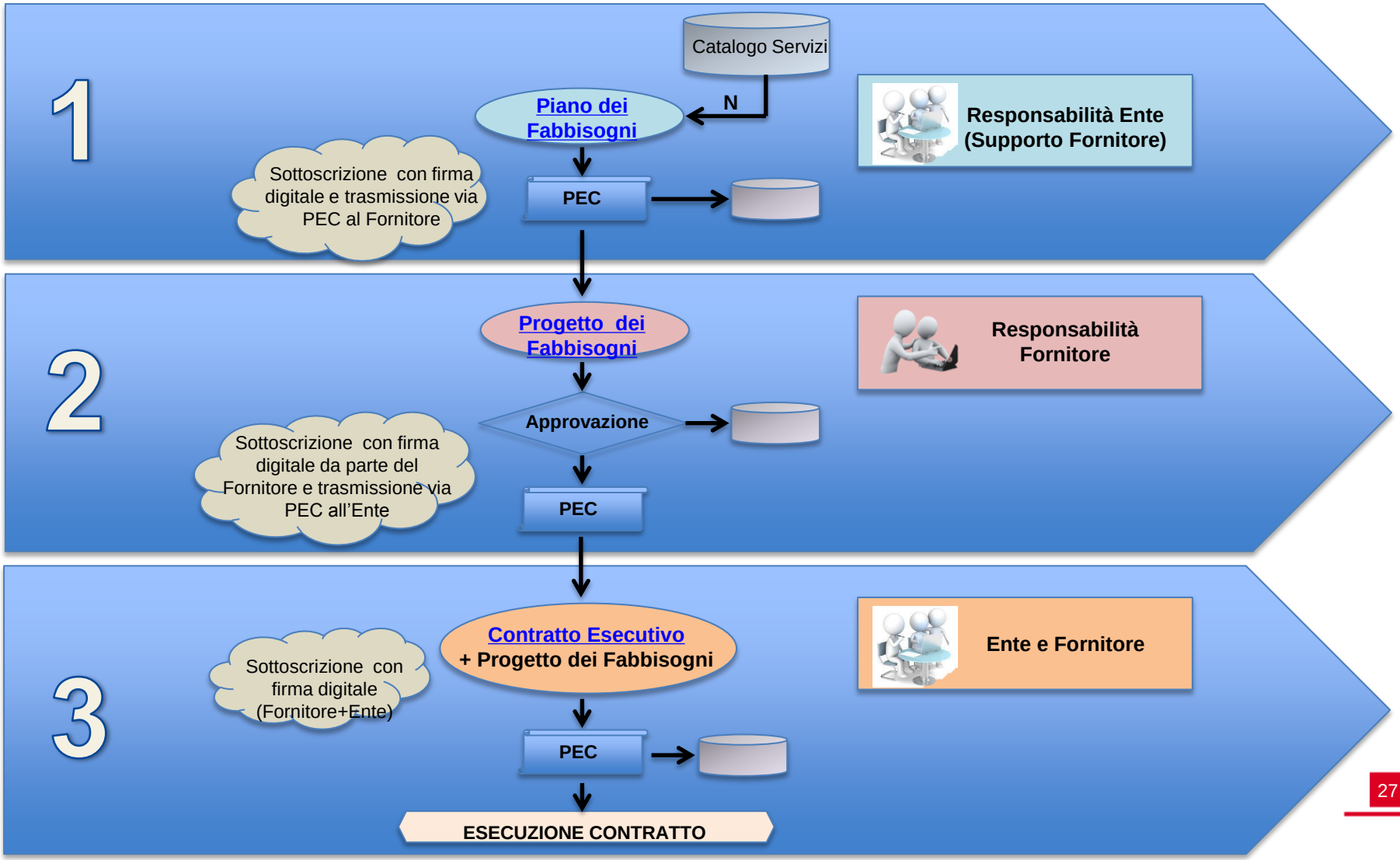
Consulting Leonardo – Data Protection Services

Schema Progetto dei Fabbisogni

Id Servizio	Titolo	Descrizione
L2.S3.9-SP1	General Data Protection Regulation Assessment	Servizi di assessment privacy per effettuare una mappatura dei trattamenti e dei ruoli al principale scopo della realizzazione del "Registro delle attività di trattamento", ai sensi dell'art.30 del GDPR.
L2.S3.9-SP2	GDPR Design	Servizi di consulenza per l'analisi, il disegno, la progettazione dei processi per la protezione dei dati in conformità al nuovo GDPR.
L2.S3.9-SP3	GDPR Implementation & Data Protection Management	Servizi di supporto all'implementazione e al mantenimento del sistema di gestione della protezione dei dati in coerenza con il nuovo GDPR.

Servizi di identità digitale e sicurezza applicativa

Adesione al Contratto Quadro – Processo



Corrado Grosso
Security & Information Systems Division
Area Nord Sales - Territory Manager

Tel.: +39 010 6583096
Mob: +39 335 6970060
corrado.grosso@leonardocompany.com
leonardocompany.com

Emanuele Rosa
Security & Information Systems Division
Cyber Services & Intelligence Business Area

Tel.: +39 0331 1753249
Mob: +39 331 6773773
emanuele.rosa@leonardocompany.com
leonardocompany.com

THANK **YOU** FOR YOUR ATTENTION

LEONARDO
SECURITY & INFORMATION SYSTEMS