GALLI DATA SERVICE

CONFINDUSTRIA PIACENZA



IL NUOVO REGOLAMENTO PRIVACY EUROPEO

DATA PROTECTION EXCHANGE

DOMANDE E RISPOSTE,
a un anno dall'entrata in vigore

24/05/2017 – ore 09,00
Confindustria Piacenza

- Martin Schulz – Il Firmatario del GDPR
- Galli Data Service – Interpretazioni, suggerimenti
- Associati – Case history, dubbi, commenti, ecc.
- ???



IL PROGRAMMA DEGLI ARGOMENTI:



1) scelta del **perimetro di applicazione**
(possibilità di impostare un unico modello su tutto il territorio europeo, interfacciandosi ad un'unica Autorità di controllo)



2) principio di **accountability**
(classificazione delle attività di trattamento, analisi dei rischi ed implementazione di adeguate misure di sicurezza)



3) **nuovi obblighi** e sistema di gestione
(gestire un presidio operativo costante sulla sicurezza dei dati in azienda per data breach, privacy by default, ecc.)



4) definizione della **governance**
(assegnare ruoli e responsabilità a tutti i soggetti, interni ed esterni, coinvolti nel trattamento; possibilità di nominare un Responsabile della Protezione dei dati o Data Protection Officer)



5) garanzie di **trasparenza** (valorizzare, tramite i propri canali informativi, l'attenzione alla tutela dei dati)

ALCUNE PREMESSE:

1) Finalità del GDPR e ambito di applicazione

- incentivare la circolazione dei dati
- tutte le organizzazioni, tutti i dati
- No trattamenti in ambito privato

2) Ratio normativa nordica

-no proroghe, interpretazioni, ecc.
- direttamente applicabile

3) Principio di **accountability**

-No "one size fits all"
-Approccio risk-based
-Pretesa di durare nel tempo

4) Apparato sanzionatorio

CAPO IV
Titolare del trattamento e responsabile del trattamento

Sezione 1
Obblighi generali

Articolo 24
Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

scelta del **perimetro di applicazione**

- Austria
- Belgio
- Bulgaria
- Cipro
- Croazia
- Danimarca
- Estonia
- Finlandia
- Francia
- Germania
- Grecia
- Irlanda
- Italia
- Lettonia
- Lituania
- Lussemburgo
- Malta
- Paesi Bassi
- Polonia
- Portogallo
- Regno Unito
- Rep. Ceca
- Romania
- Slovacchia
- Slovenia
- Spagna
- Svezia
- Ungheria



Principio di **accountability**

1 **CLASSIFICAZIONE DEI DATI**
(Registri delle attività di trattamento, Art.30)
DOVE SONO I DATI NELLA MIA ORGANIZZAZIONE?

2 **VALUTAZIONE DI RISCHIO**
(Sicurezza del trattamento, Art.32)
QUALI CRITICITA' PRIVACY COMPORTANO?

3 **PROTEZIONE DEI DATI**
(Sicurezza del trattamento, Art. 32)
QUALI MISURE DI SICUREZZA IMPLEMENTO?

Principio di **accountability**

1 CLASSIFICAZIONE DEI DATI

(Registri delle attività di trattamento, Art.30)
DOVE SONO I DATI NELLA MIA ORGANIZZAZIONE?

CONSIGLI:

- Classificare per funzione (HR, AMM, COMM, MKT, LOG, …)
- Classificare per applicativi e strumenti
  (PC, Share di rete, Device, Sito, Videosorveglianza, ecc.)
- Valutare dati critici per business e know-how

Principio di **accountability**

2 RISK ASSESSMENT

(Valutazione di impatto sui diritti e le libertà degli interessati)

STANDARD UNI ISO 31.000 - Valutazione "a sentimento"

CONSIGLIO:

- Definire una metodologia (anche semplice) basata su parametri oggettivi e misurabili

Principio di **accountability**

2 RISK ASSESSMENT
(Valutazione di impatto sui diritti e le libertà degli interessati)

SUGGERIMENTI CONSIDERANDO GARANTE

[ ] Possibile fonte di discriminazioni
[ ] Possibile furto o usurpazione identità
[ ] Causa di perdite finanziarie
[ ] Causa di pregiudizio alla reputazione
[ ] Danno economico / sociale significativo
[ ] Privazione di diritti e libertà fondamentali
[ ] Trattamento di dati sensibili
[ ] Trattamento di profilazione
[ ] Dati di minori
[ ] Dati coperti da segreto professionale
[ ] Ampiezza banca dati

Principio di **accountability**

2 RISK ASSESSMENT
(Valutazione di impatto sui diritti e le libertà degli interessati)

SUGGERIMENTI ENISA

LEVEL OF IMPACT	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Principio di **accountability**

3

PROTEZIONE DEI DATI

(Sicurezza del trattamento, Art. 32)
QUALI MISURE DI SICUREZZA IMPLEMENTO?

CONSIGLI:

- Definire il giusto mix di misure tecniche, organizzative, fisiche, ecc. (es: accesso logico, segragation of duties, log-management, protezione malware e perimetrale, patching, back-up/recovery/continuity, cifratura, anonimizzazione, vulnerability assessment, penetration testing, controllo accessi, videosorveglianza, vigilanza, nomine, istruzioni, clausole contrattuali, ecc.)

- Formazione intelligente

Nuovi obblighi e **sistema di gestione**

- **DATA BREACH – Art.33 GDPR**
  (gestione incidenti di sicurezza)
  TIMING: immediata documentazione, entro 72 ore notifica

- **PRIVACY BY DESIGN – Art.25 GDPR**
  (nuovi processi, nuove tecnologie, nuovi incaricati)
  TIMING: prima dell'inizio del trattamento

- **PRIVACY IMPACT ASSESSMENT – Art. 35 GDPR**
  (approfondimenti su trattamenti critici)
  TIMING: prima dell'inizio del trattamento

- **DIRITTO ACCESSO – Art.15 GDPR**
  (Rispondere a richieste degli interessati)
  TIMING: Entro 1 mese

- **RACCOLTA DATI PRESSO TERZI – Art.14**
  (Informativa agli interessati)
  TIMING: Entro 1 mese

FLUSSO INFORMATIVO COSTANTE:

- ALLERT REFERENTI
- REMINDER PERIODICI
- AUDIT PERIODICI

Definizione **governance**

Art. 4, comma7 – Art. 24

- **TITOLARE DEL TRATTAMENTO**

Art.4, comma 8 – Art. 28

- **RESPONSABILE DEL TRATTAMENTO**

Art.26 Cotitolare del trattamento

Art. 27 Rappresentante su territorio UE

Art. 37

- **Responsabile della Protezione dei Dati / Data Protection Officer**

QUALI SONO I REQUISITI?

Il Responsabile della protezione dei dati personali, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

1. possedere un'**adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**;
2. adempiere alle sue funzioni in **piena indipendenza** ed in assenza di **conflitti di interesse**;
3. operare **alle dipendenze del titolare o del responsabile** oppure sulla base di **un contratto di servizio**.

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati personali le **risorse umane e finanziarie** necessarie all'adempimento dei suoi compiti.

QUALI SONO I COMPITI?

Il Responsabile della protezione dei dati personali dovrà:

a) **informare e consigliare** il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli **obblighi derivanti dal Regolamento europeo** e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) **verificare l'attuazione e l'applicazione del Regolamento**, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli *audit* relativi;

c) **fornire**, se richiesto, **pareri** in merito alla **valutazione d'impatto** sulla protezione dei dati e sorvegliare i relativi adempimenti;

d) **fungere da punto di contatto** per gli **interessati** in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;

e) **fungere da punto di contatto** per il **Garante per la protezione dei dati personali** oppure, eventualmente, consultare il Garante di propria iniziativa.

Definizione
governance

ALRI SOGGETTI: Articolo 29 "Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento"

Il responsabile del trattamento, o ***chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento****, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento*

- REFERENTI PRIVACY
- AMM.TORI DI SISTEMA
- IMPIEGATI CON STRUMENTI ELETTRONICI INDIVIDUALI
- OPERAI CON STRUMENTI ELETTRONICI CONDIVISI
- OPERAI SENZA STRUMENTI ELETTRONICI

Valutare nomina, attività, istruzioni/formazione, monitoraggio

Obblighi
trasparenza

Contenuti dell'informativa

I contenuti dell'informativa sono elencati **in modo tassativo** negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare **DEVE SEMPRE** specificare i **dati di contatto del RPD-DPO**, ove esistente, la **base giuridica** del trattamento, **qual è il suo interesse legittimo** se quest'ultimo costituisce la base giuridica del trattamento, nonché **se trasferisce i dati personali in Paesi terzi** e, in caso affermativo, **attraverso quali strumenti** (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.). Il regolamento prevede anche **ulteriori informazioni** in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare **il periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di **presentare un reclamo** all'autorità di controllo. Se il trattamento comporta processi decisionali automatizzati (anche la **profilazione**), l'informativa deve specificarlo e deve indicare anche la **logica** di tali processi decisionali e le conseguenze previste per l'interessato.

Modalità dell'informativa

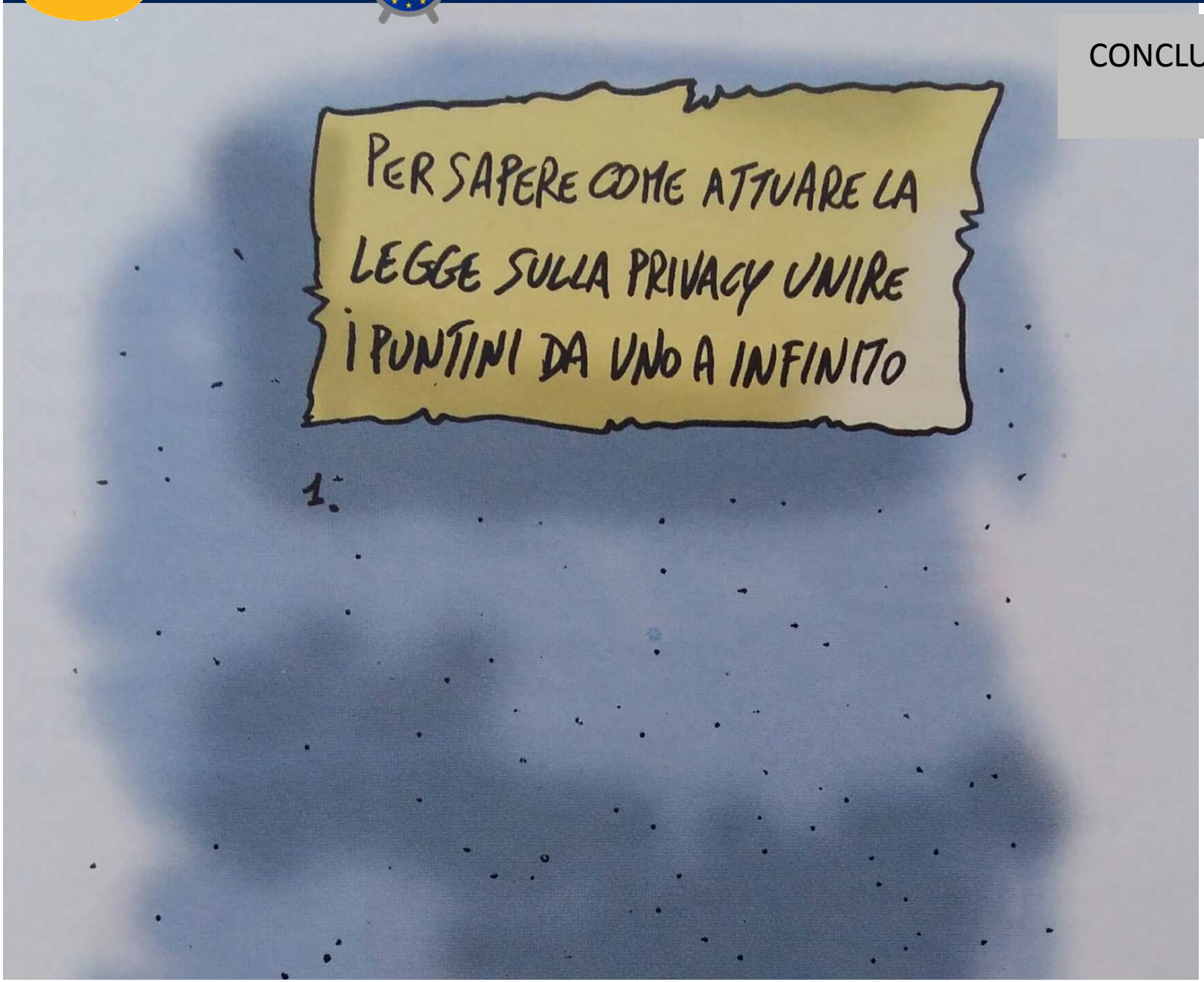
Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee *(si veda anche considerando 58)*. L'informativa è data, **in linea di principio, per iscritto** e **preferibilmente in formato elettronico** (soprattutto nel contesto di servizi online: *si vedano art. 12, paragrafo 1, e considerando 58*), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra *(art. 12, paragrafo 1)*. Il regolamento ammette, soprattutto, l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "in combinazione" con l'informativa estesa** *(art. 12, paragrafo 7)*; queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.

EVIDENZE SUI PRINCIPI GENERALI CHE IL TITOLARE E' CHIAMATO A DIMOSTRARE

Obblighi
trasparenza

- Art. 15 Diritto di accesso
- Art. 16 Diritto di rettifica
- Art. 17 Diritto di cancellazione (Diritto all'oblio)
- Art. 18 Diritto alla limitazione
- Art. 20 Diritto alla portabilità
- Art. 21 Diritto di opposizione

CONCLUSIONI



CONCLUSIONI

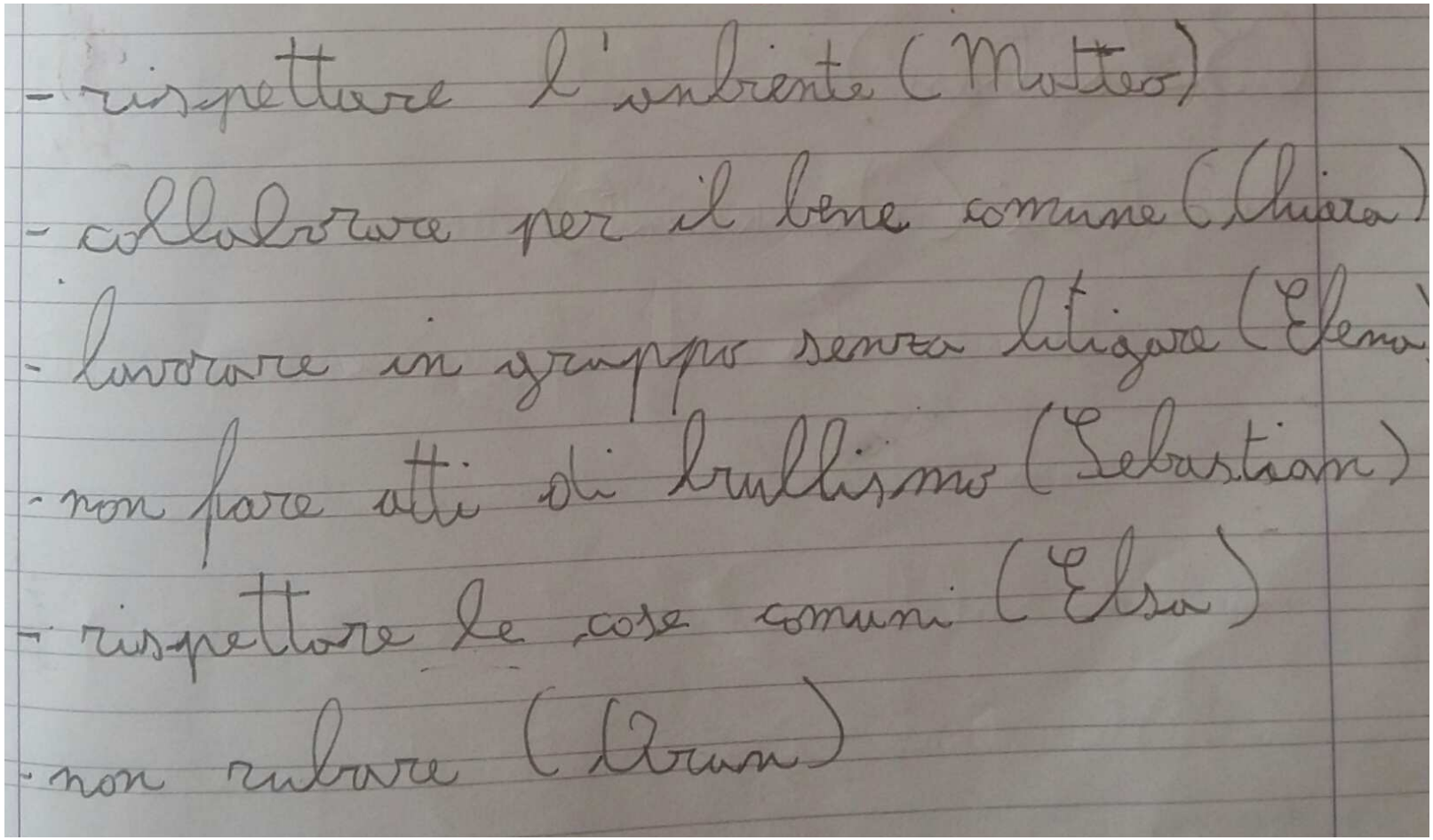
PERIMETRO	•Definire i confini di applicaiozne del Modello •Definire flussi internazionali dati
GOVERNANCE	•Definire ruoli e responsbailità •(Data controller, data processor, data protection officer, comitato privacy, referenti funzione, outsourcer critici, incaricati, ecc.)
CONSAPEVOLEZZA	•Attivare strumenti di informazione, condivisione flussi, coinvolgimento management, sensiblizzazione del personale, formazione mirata per funzioni critiche, formazione etsesa su rischi
ACCOUNTABILITY	•Implementare politiche di sicurezza personalizzate, basate su "data inventory" - privacy impact assesment (rischio) - misure adeguate •(eventuale tutela dati know-how e business)
SISTEMA DOCUMENTALE	•Documentare le scelte di compliance in modo significativo e personalizzato, al fine di presidiare il sistema e predisporre un fascicolo completo opponibile a terzi proposti a controlli
SISTEMA DI GESTIONE	•Prevedere la ripetizione ciclica (secondo la logica PDCA) delle fasi di progettazione, attuazione, verifica e miglioramento del sistema •Programmazione di audit ed aggiornamenti periodici

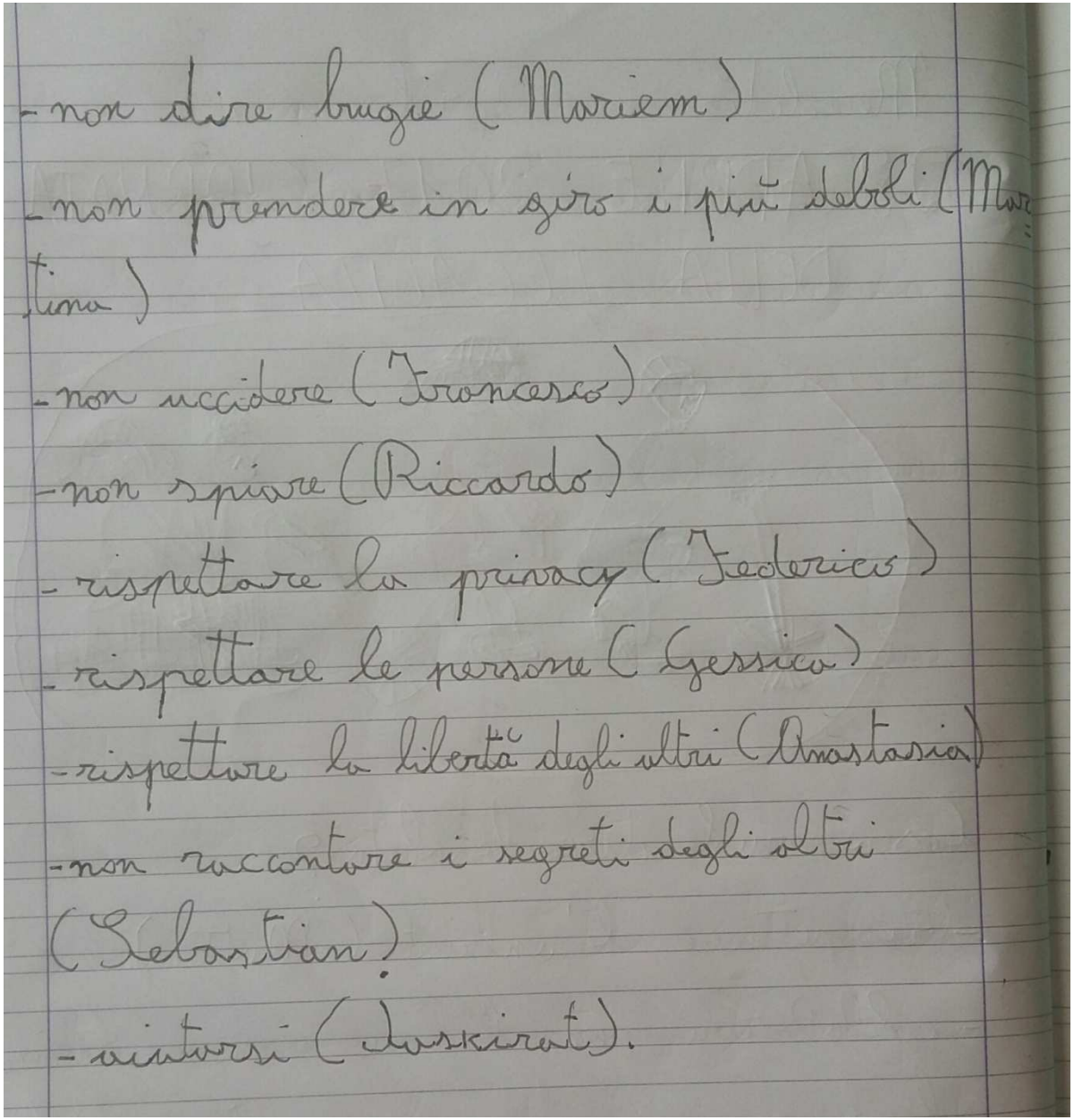
CONFORMITA' PRIVACY EUROPEA

VALORI AGGIUNTI




Mercoledì 12 Aprile 2017
28 APRILE 2017 GIORNATA
DELLA LEGALITÀ
Cosa vuol dire legalità?


- rispettare l'ambiente (Matteo)
- collaborare per il bene comune (Chiara)
- lavorare in gruppo senza litigare (Elena)
- non fare atti di bullismo (Sebastian)
- rispettare le cose comuni (Elsa)
- non rubare (Bruno)



- non dire bugie (Mariem)
- non prendere in giro i più deboli (Mar
tina)
- non uccidere (Francesco)
- non spiare (Riccardo)
- rispettare la privacy (Federico)
- rispettare le persone (Jessica)
- rispettare la libertà degli altri (Anastasia)
- non raccontare i segreti degli altri
(Sebastian)
- aiutarsi (Juskiraf).

Grazie per l'attenzione!

www.gallidataservice.com