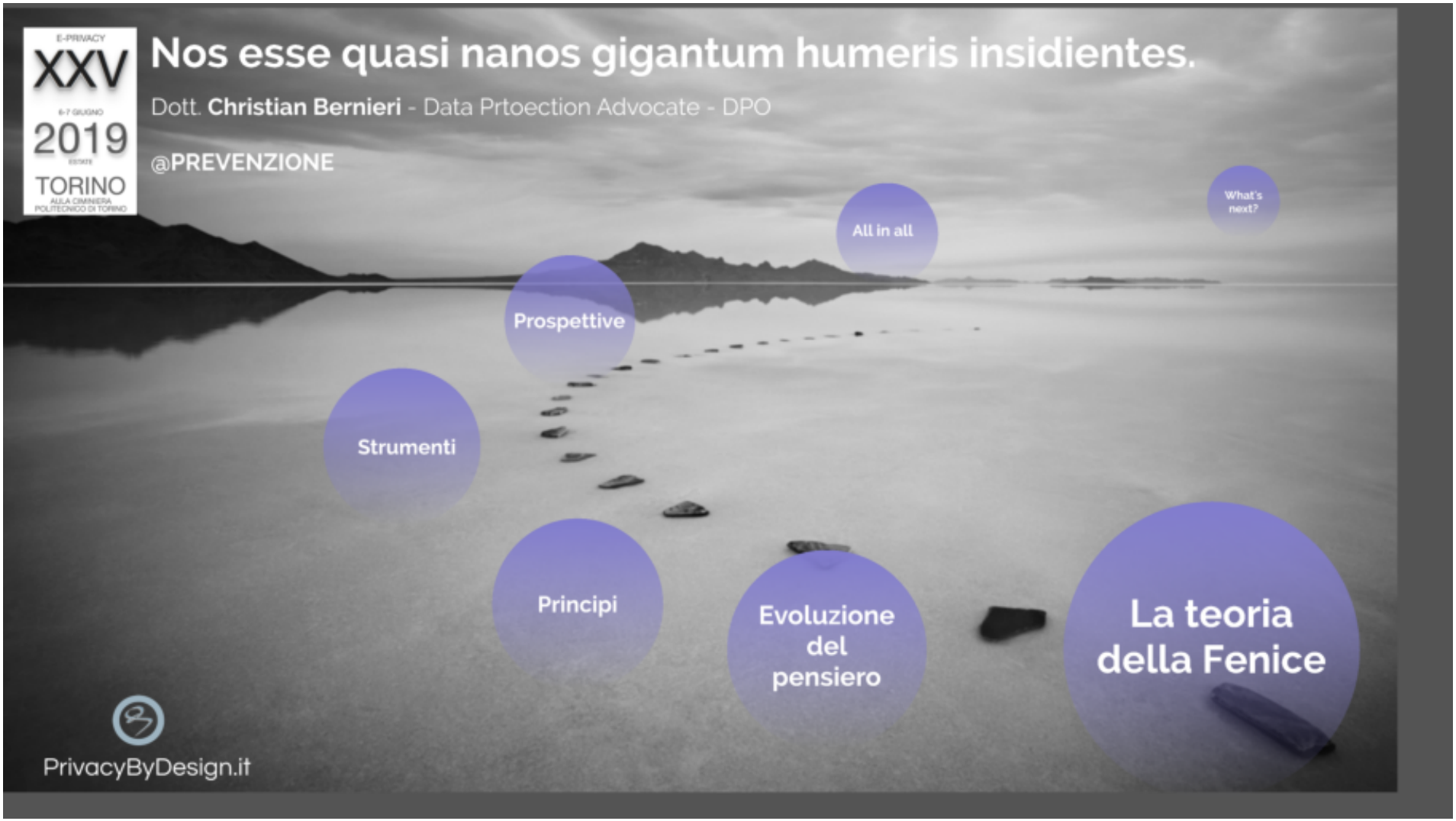
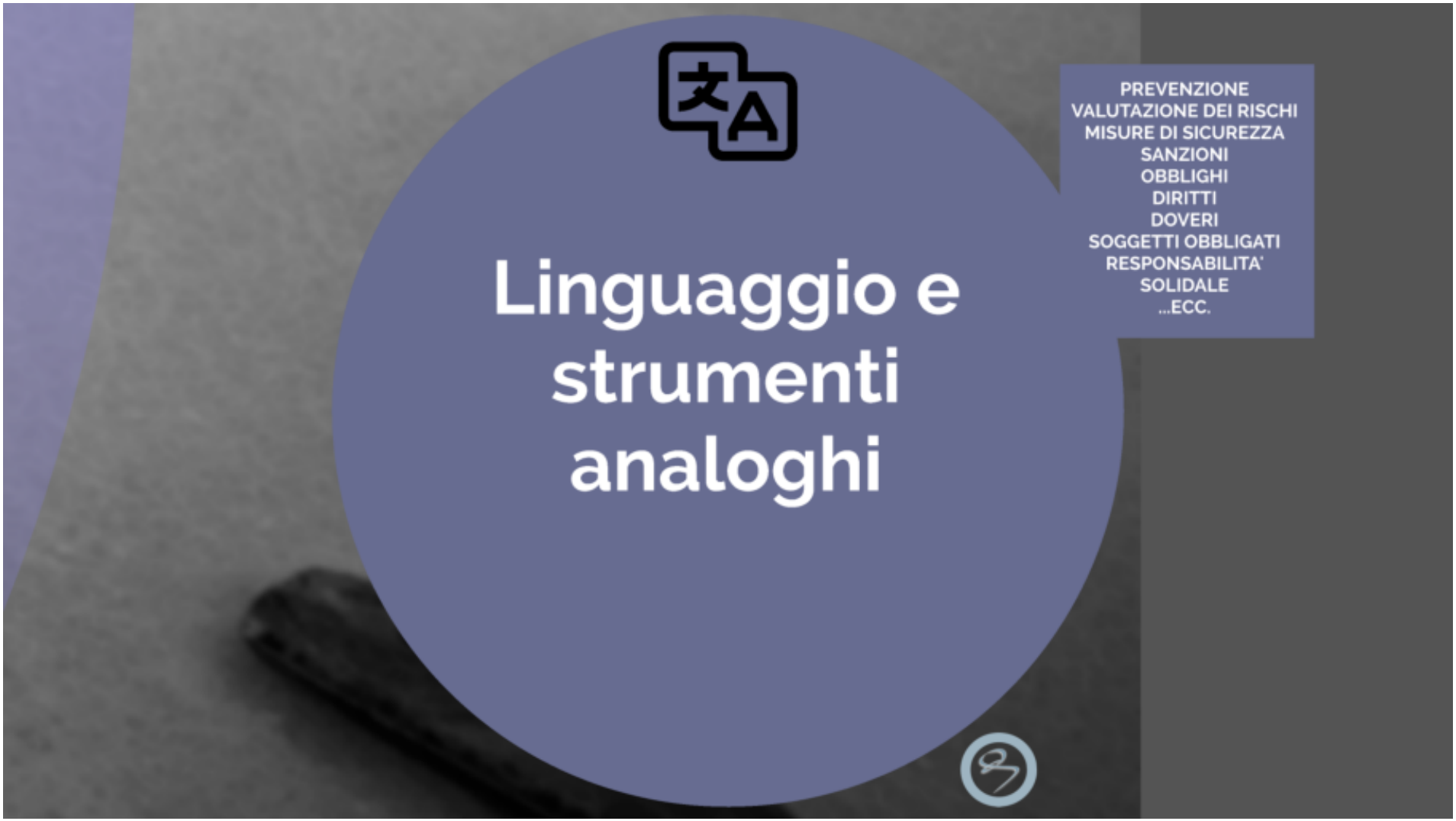

E-PRIVACY
XXV
6-7 GIUGNO
2019
EDIZIONE
TORINO
AULA CIMINIERA
POLITECNICO DI TORINO
Nos esse quasi nanos gigantum humeris insidientes.
Dott. Christian Bernieri - Data Prtoection Advocate - DPO
@PREVENZIONE
What's next?
All in all
Prospettive
Strumenti
Principi
Evoluzione del pensiero
La teoria della Fenice
PrivacyByDesign.it

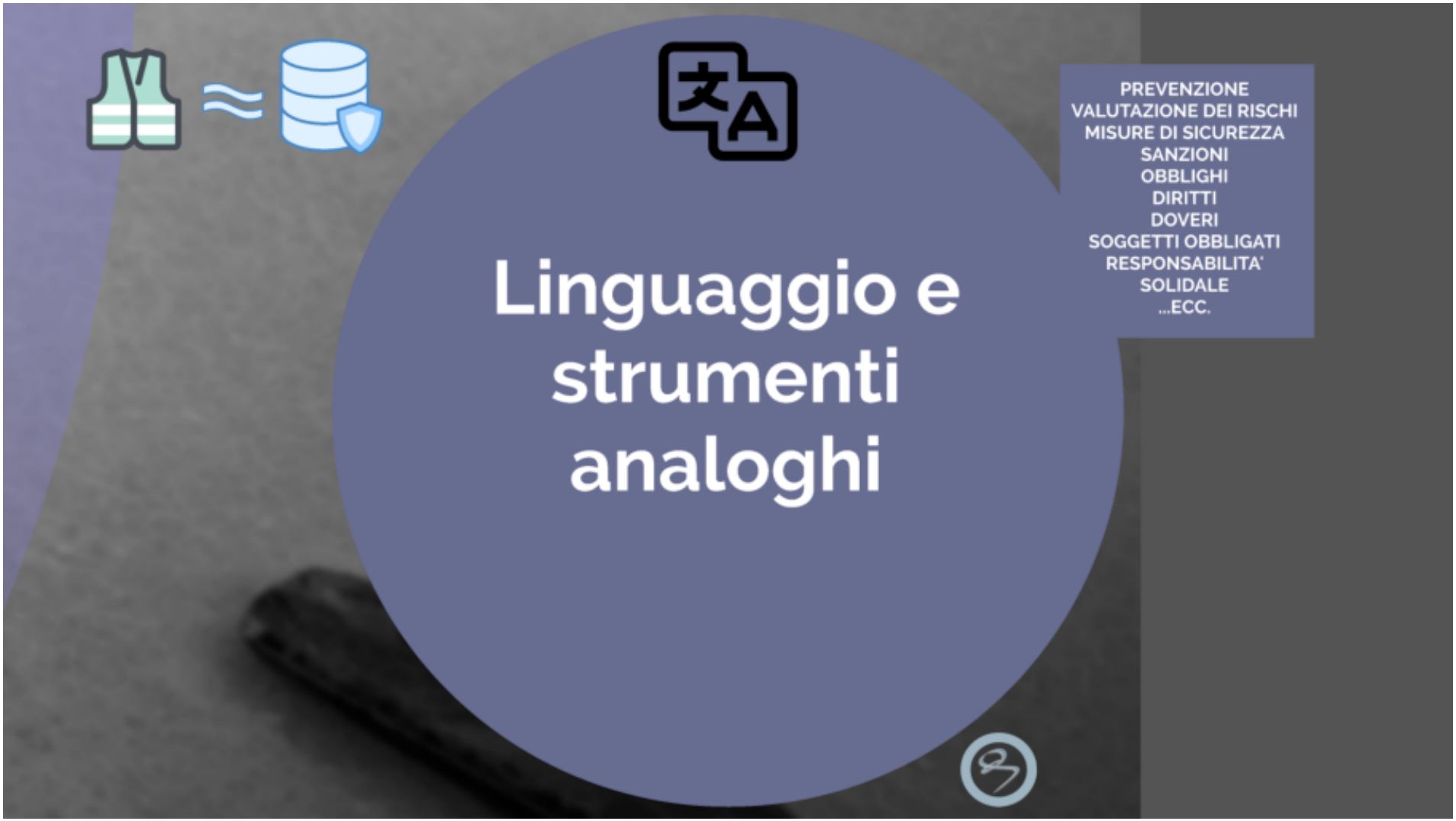

La teoria della Fenice
la **protezione dei dati *(DP)*** può iniziare il suo cammino da dove si è arrivati in ambito di **sicurezza del lavoro *(HeS)***.
Cosa significa?
1
DIRITTI FONDAMENTALI
2
LINGUAGGIO
3
RISVOLTI PRATICI
4


La teoria della fenice
La protezione dei dati (DP) è una materia relativamente nuova rispetto alla salute e alla sicurezza sul lavoro (HeS).
Molti strumenti utilizzati per garantire la privacy sono nuovi e creativi, ma, visto dal punto di vista del know-how HeS, si può dire che tutti i professionisti della privacy stiano percorrendo una strada già nota.
Esamineremo alcuni degli strumenti e soluzioni (classiche o innovative) che si ritrovano già nelle buone prassi e nelle norme in materia di HeS.
Molti altri strumenti possono essere adattati alla DP. Guardando all'evoluzione di HeS e alle sue nuove frontiere possiamo accelerare l'evoluzione della protezione dei dati.


SICUREZZA DEL LAVORO
Garantire la **salute** e **sicurezza** in ambito lavorativo rispetto al rischio di infortunio o malattia.
PROTEZIONE DEI DATI
Garantire la **libertà** degli individui attraverso il governo dei dati personali, in tutti gli ambiti di vita.

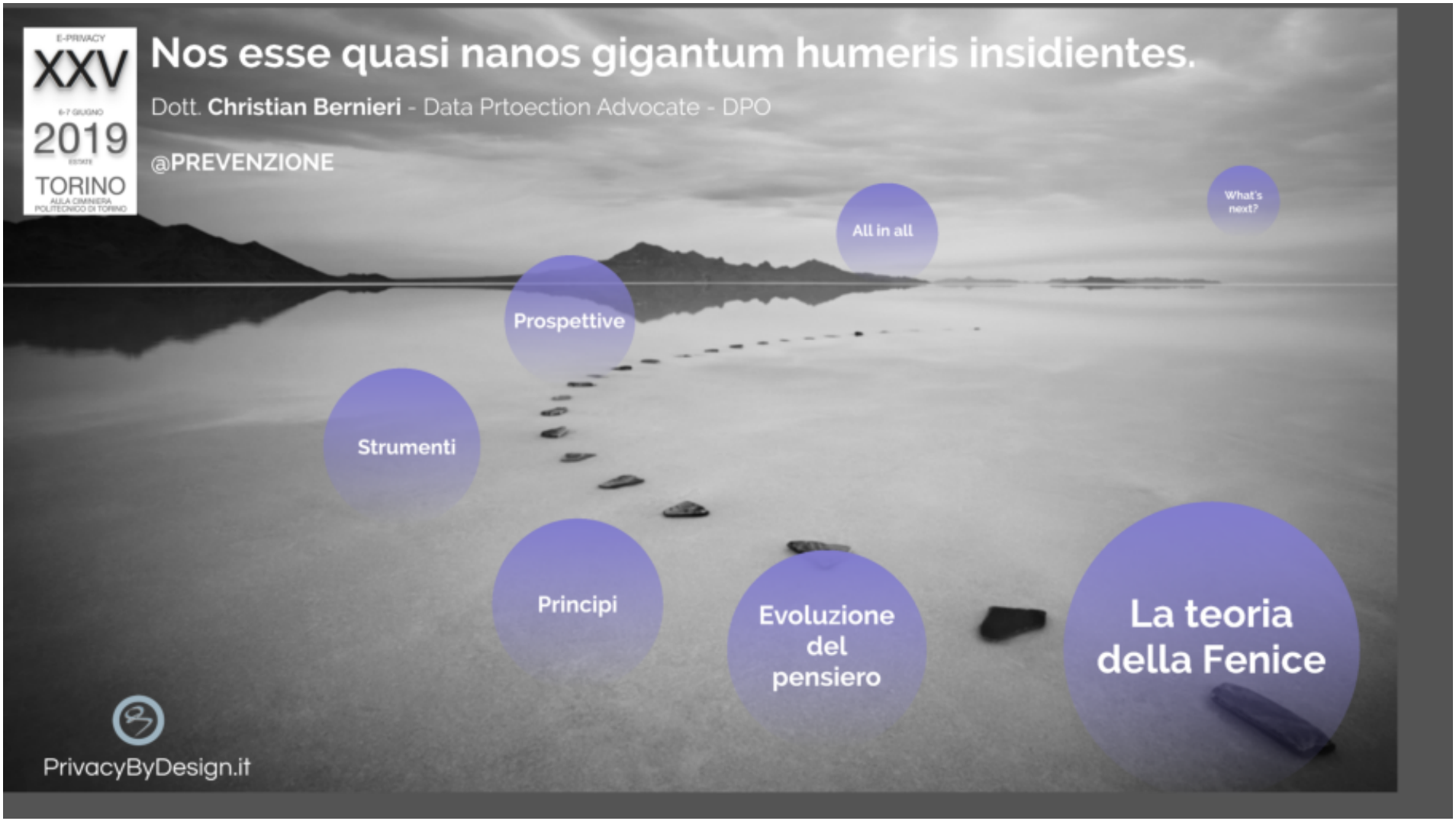

SICUREZZA DEL LAVORO
Garantire la **salute** e **sicurezza** in ambito lavorativo rispetto al rischio di infortunio o malattia.
PROTEZIONE DEI DATI
Garantire la **libertà** degli individui attraverso il governo dei dati personali, in tutti gli ambiti di vita.

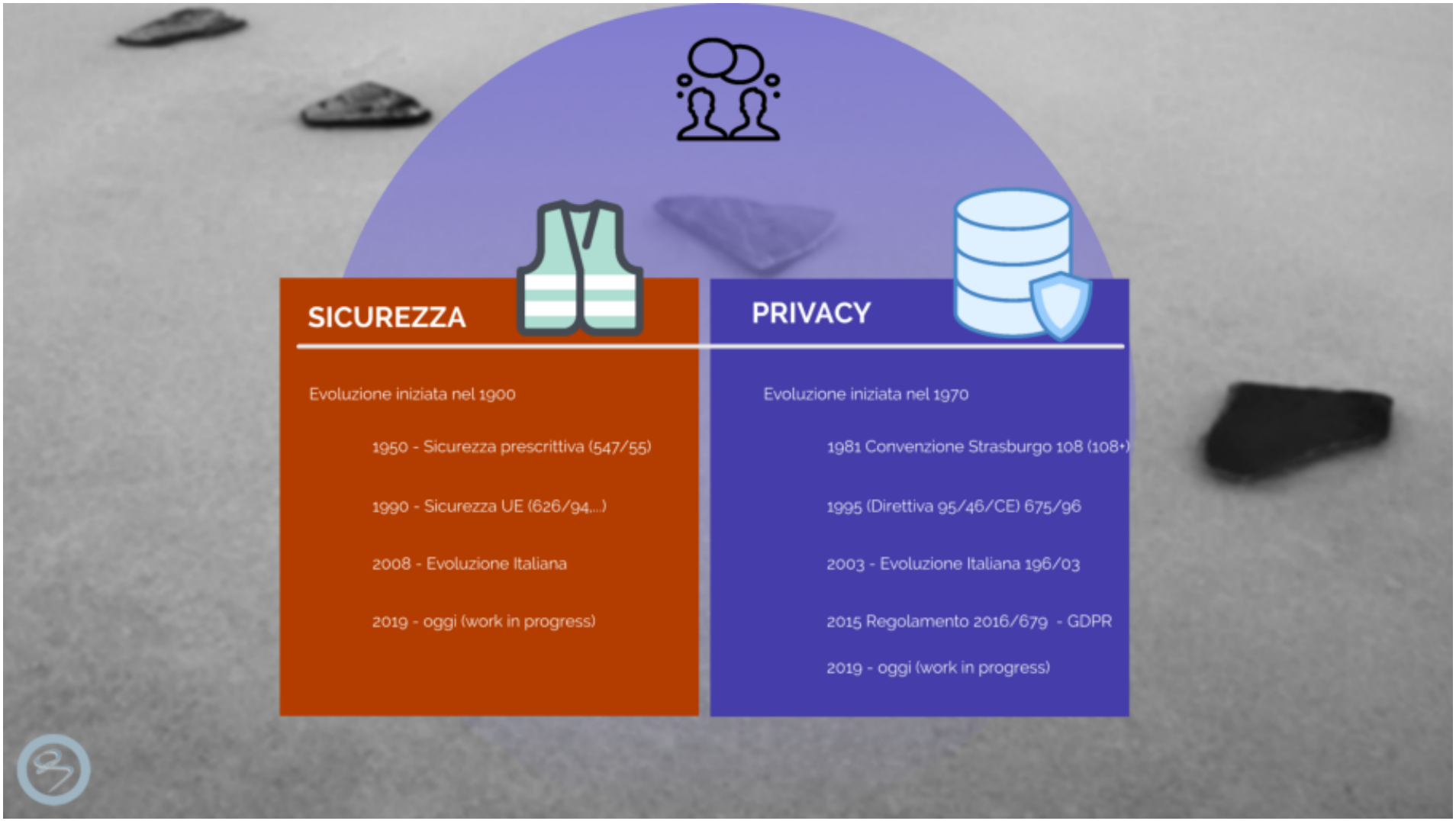

Linguaggio e strumenti analoghi
PREVENZIONE
VALUTAZIONE DEI RISCHI
MISURE DI SICUREZZA
SANZIONI
OBBLIGHI
DIRITTI
DOVERI
SOGGETTI OBBLIGATI
RESPONSABILITA'
SOLIDALE
...ECC.


Linguaggio e strumenti analoghi
PREVENZIONE
VALUTAZIONE DEI RISCHI
MISURE DI SICUREZZA
SANZIONI
OBBLIGHI
DIRITTI
DOVERI
SOGGETTI OBBLIGATI
RESPONSABILITA'
SOLIDALE
...ECC.


Vantaggi...


Uniformità
Rapidità
Risparmio
Compliance


E-PRIVACY
XXV
6-7 GIUGNO
2019
EDIZIONE
TORINO
AULA CIMINIERA
POLITECNICO DI TORINO
Nos esse quasi nanos gigantum humeris insidientes.
Dott. Christian Bernieri - Data Prtoection Advocate - DPO
@PREVENZIONE
What's next?
All in all
Prospettive
Strumenti
Principi
Evoluzione del pensiero
La teoria della Fenice
PrivacyByDesign.it


SICUREZZA
Evoluzione iniziata nel 1900
1950 - Sicurezza prescrittiva (547/55)
1990 - Sicurezza UE (626/94...)
2008 - Evoluzione Italiana
2019 - oggi (work in progress)
PRIVACY
Evoluzione iniziata nel 1970
1981 Convenzione Strasburgo 108 (108+)
1995 (Direttiva 95/46/CE) 675/96
2003 - Evoluzione Italiana 196/03
2015 Regolamento 2016/679 - GDPR
2019 - oggi (work in progress)

SICUREZZA

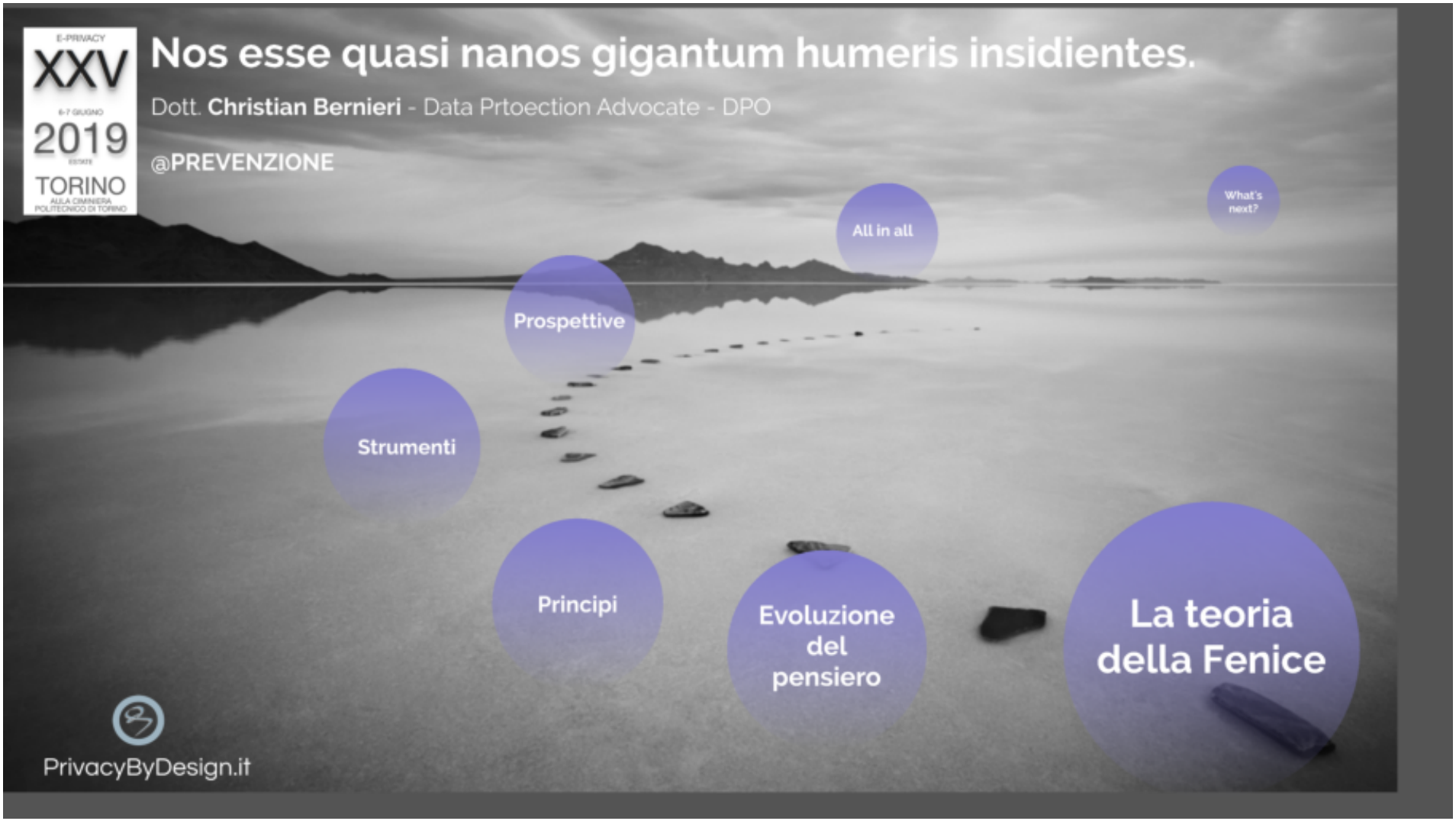
Evoluzione iniziata nel 1900

- 1950 - Sicurezza prescrittiva (547/55)
- 1990 - Sicurezza UE (626/94,...)
- 2008 - Evoluzione Italiana
- 2019 - oggi (work in progress)

PRIVACY

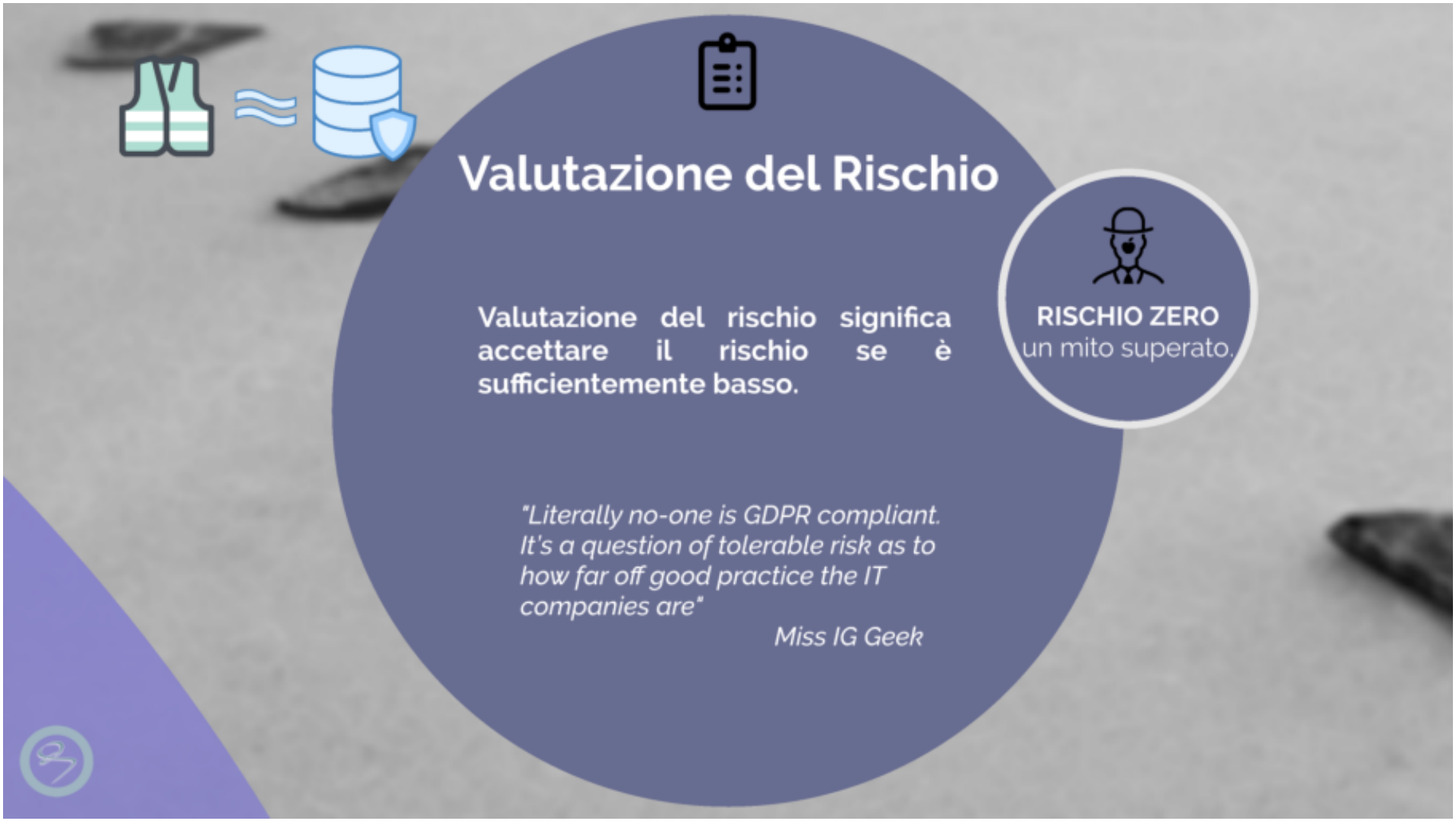
Evoluzione iniziata nel 1970

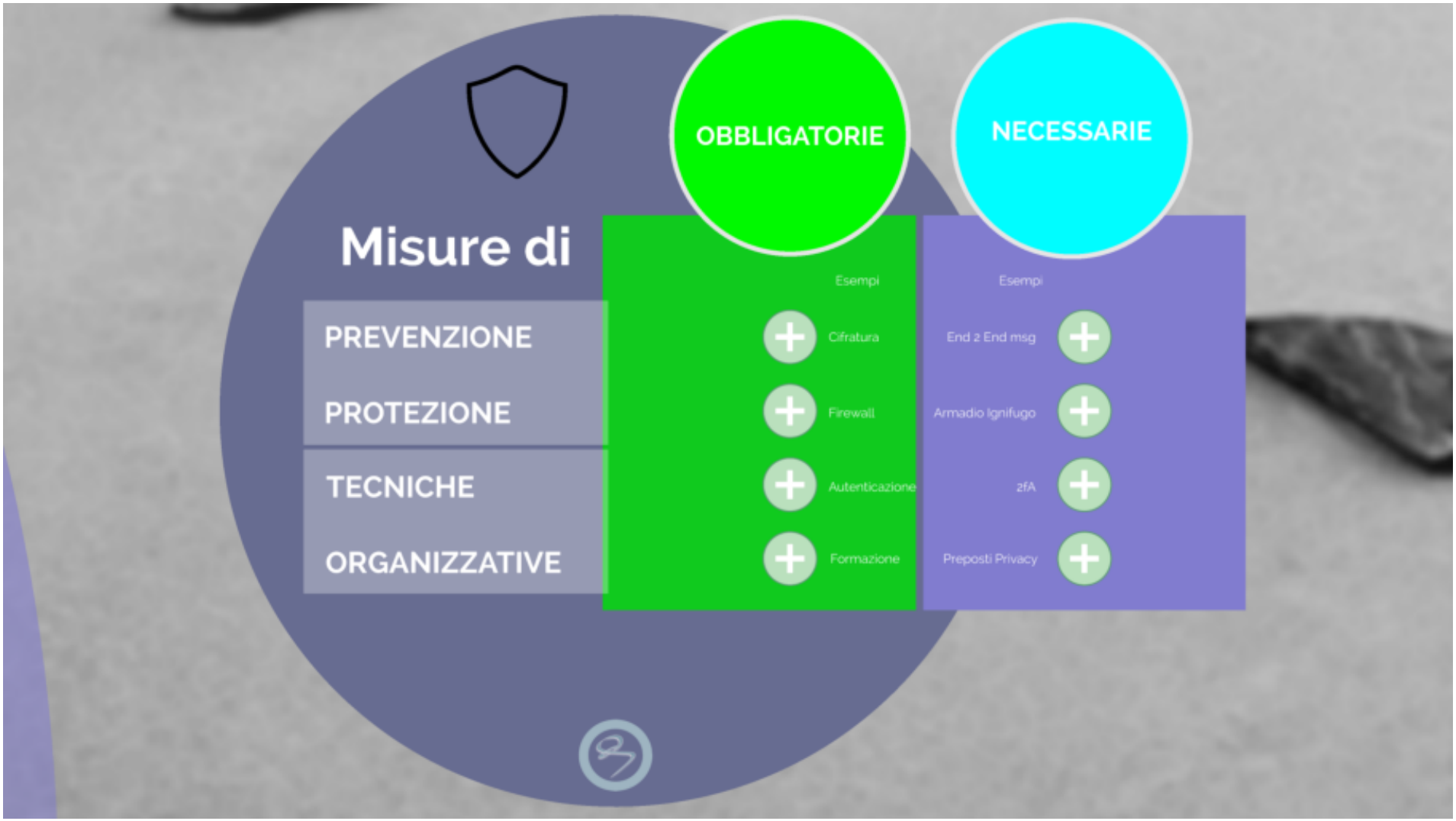
- 1981 Convenzione Strasburgo 108 (108+)
- 1995 (Direttiva 95/46/CE) 675/96
- 2003 - Evoluzione Italiana 196/03
- 2015 Regolamento 2016/679 - GDPR
- 2019 - oggi (work in progress)

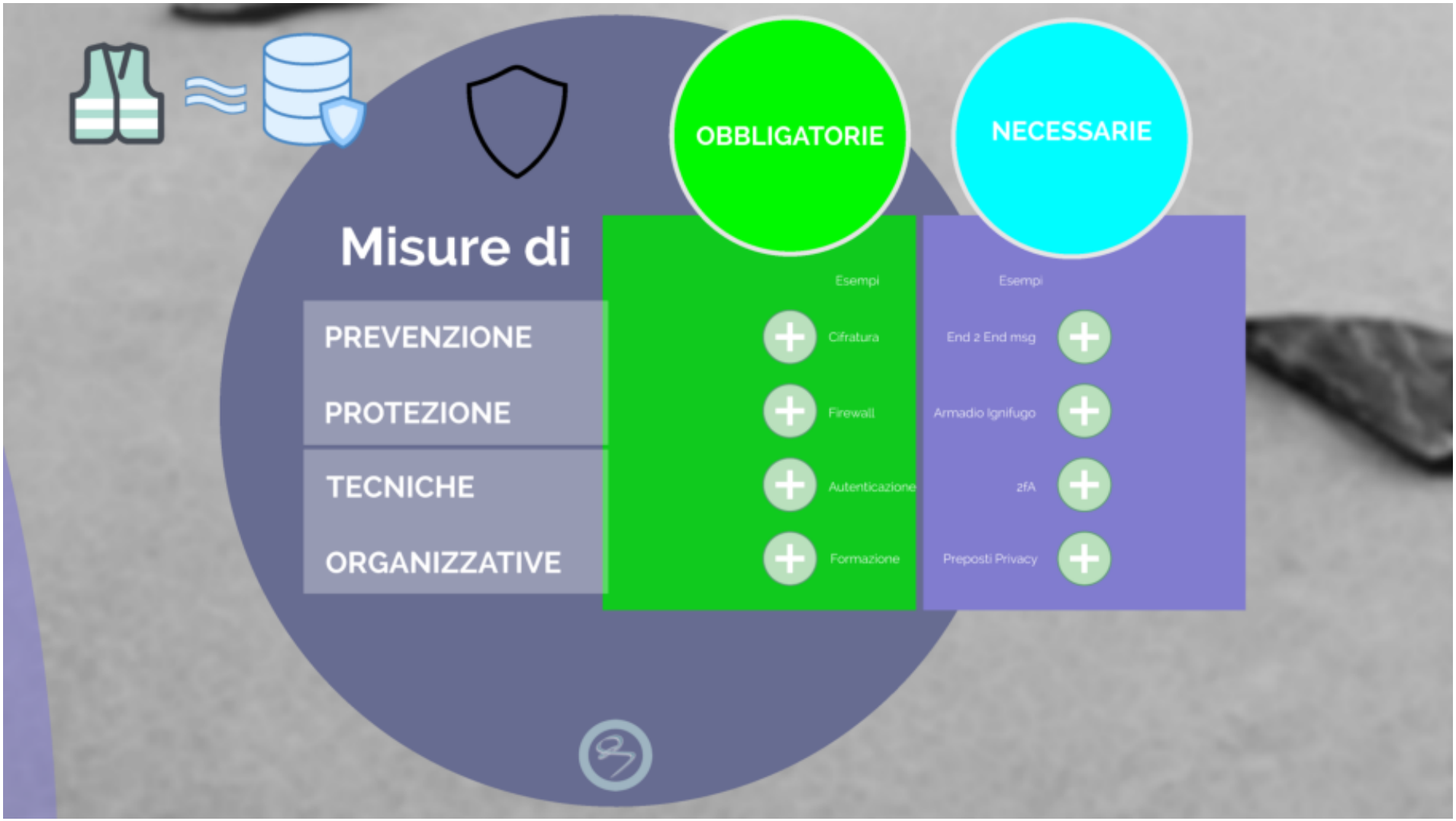

E-PRIVACY
XXV
6-7 GIUGNO
2019
TORINO
AULA CIMINIERA
POLITECNICO DI TORINO
Nos esse quasi nanos gigantum humeris insidientes.
Dott. Christian Bernieri - Data Prtoection Advocate - DPO
@PREVENZIONE
What's next?
All in all
Prospettive
Strumenti
Principi
Evoluzione del pensiero
La teoria della Fenice
PrivacyByDesign.it


Principi comuni tra HeS e DP
I punti di contatto tra le discipline sono spesso i fondamenti stessi per l'applicazione delle norme.
VDR come processo
Misure
Stato dell'arte
Responsabilità


Valutazione del Rischio
Valutazione del rischio significa accettare il rischio se è sufficientemente basso.
RISCHIO ZERO
un mito superato.
"Literally no-one is GDPR compliant. It's a question of tolerable risk as to how far off good practice the IT companies are"
Miss IG Geek


Valutazione del Rischio
Valutazione del rischio significa accettare il rischio se è sufficientemente basso.
RISCHIO ZERO
un mito superato.
"Literally no-one is GDPR compliant. It's a question of tolerable risk as to how far off good practice the IT companies are"
Miss IG Geek


Misure di
PREVENZIONE
PROTEZIONE
TECNICHE
ORGANIZZATIVE
OBBLIGATORIE
NECESSARIE
Esempi
Cifratura
Firewall
Autenticazione
Formazione
Esempi
End 2 End msg
Armadio Ignifugo
2fA
Preposti Privacy


OBBLIGATORIE
NECESSARIE
Misure di
PREVENZIONE
PROTEZIONE
TECNICHE
ORGANIZZATIVE
Esempi
Cifratura
Firewall
Autenticazione
Formazione
Esempi
End 2 End msg
Armadio Ignifugo
2fA
Preposti Privacy

Misure Obbligatorie

Provvedimento su data breach - 4 aprile 2019
... 2) l'accertata ***condivisione delle credenziali di autenticazione da parte di più incaricati****... nel previgente ordinamento erano addirittura qualificate come misure minime di sicurezza (cfr. regole nn. 2, 3 e 13 del disciplinare tecnico di cui all'****allegato B del Codice)*** *che i titolari del trattamento* ***erano tenuti ad adottare al fine di assicurare un livello minimo*** *di protezione dei dati personali.*
E' pertanto evidente come la mancata adozione di tali misure e.... rappresentino una violazione dell'obbligo di predisposizione, da parte del responsabile del trattamento, di misure tecniche e organizzative adeguate.


Misure Necessarie


Lo Stato dell'arte
è obbligatorio !
Da ultimo, il provvedimento del G.P relativo a piattaforma Rousseau: è sanzionata l'obsolescienza tecnologica (no patch) come mancanza di misura minima di prevenzione.
La sicurezza del lavoro conosce questo pincipio dal 1942.
DP
HeS

Obsolescenza nel mondo Privacy

Provvedimento su data breach - 4 aprile 2019

*Tale circostanza rende estremamente difficoltoso il patching dei sistemi online realizzati sulla piattaforma Cms, l'a**dozione di accorgimenti ad hoc e l'intervento, realisticamente non tempestivo, di sviluppatori in grado di apportare le correzioni necessarie a fronte di future vulnerabilità la cui scoperta non può essere esclusa**, come per ogni sistema software complesso, ma che in questo caso potrebbe avere un impatto particolarmente gravoso stante l'assenza di supporto ufficiale da parte del produttore.*

...

*3. entro il termine di 120 giorni dalla ricezione del presente provvedimento, ai fini del rispetto del **principio di responsabilizzazione** di cui all'articolo 24 del Regolamento, ad una rivisitazione complessiva delle iniziative di sicurezza adottate (cfr. par. 3.1 sulle **"Attività di vulnerability assessment"**),alcune delle quali, **per quanto conformi, in termini di stretto adempimento, alle prescrizioni di cui al par. 7, lett. A del provvedimento n. 548 del 2017, risultano comunque inficiate nella loro efficacia dalle gravi limitazioni tecniche intrinseche al sistema utilizzato** (CMS - Movable Type 4). L'eventuale inosservanza del presente ordine è soggetta alla sanzione amministrativa prevista dall'art. **83, par. 5, lett. e)** del Regolamento;*

Obsolescenza nel mondo Privacy

Provvedimento su data breach - 4 aprile 2019

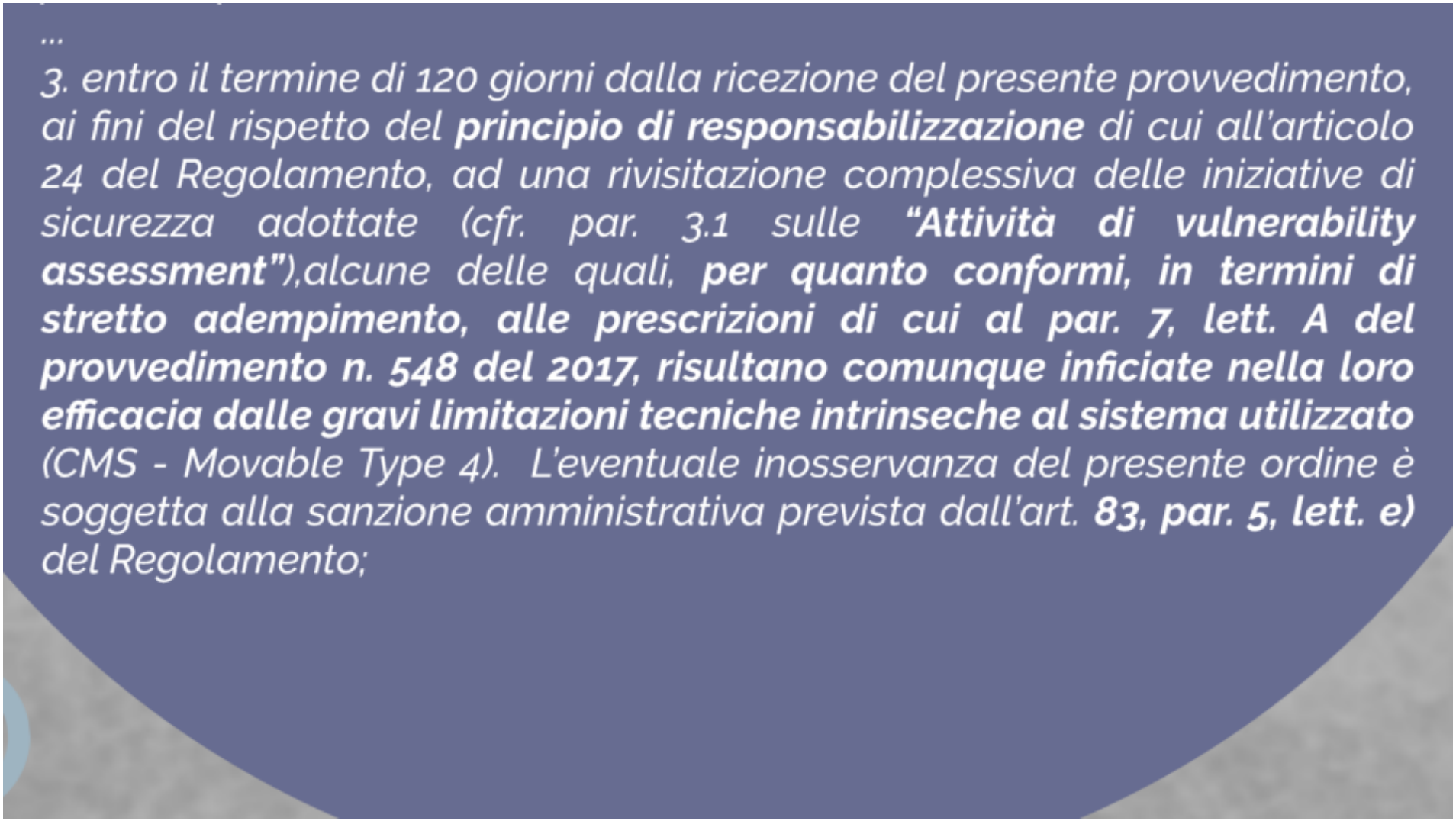
*Tale circostanza rende estremamente difficoltoso il patching dei sistemi online realizzati sulla piattaforma Cms, l'a**dozione di accorgimenti ad hoc e l'intervento, realisticamente non tempestivo, di sviluppatori in grado di apportare le correzioni necessarie a fronte di future vulnerabilità la cui scoperta non può essere esclusa**, come per ogni sistema software complesso, ma che in questo caso potrebbe avere un impatto particolarmente gravoso stante l'assenza di supporto ufficiale da parte del produttore.*

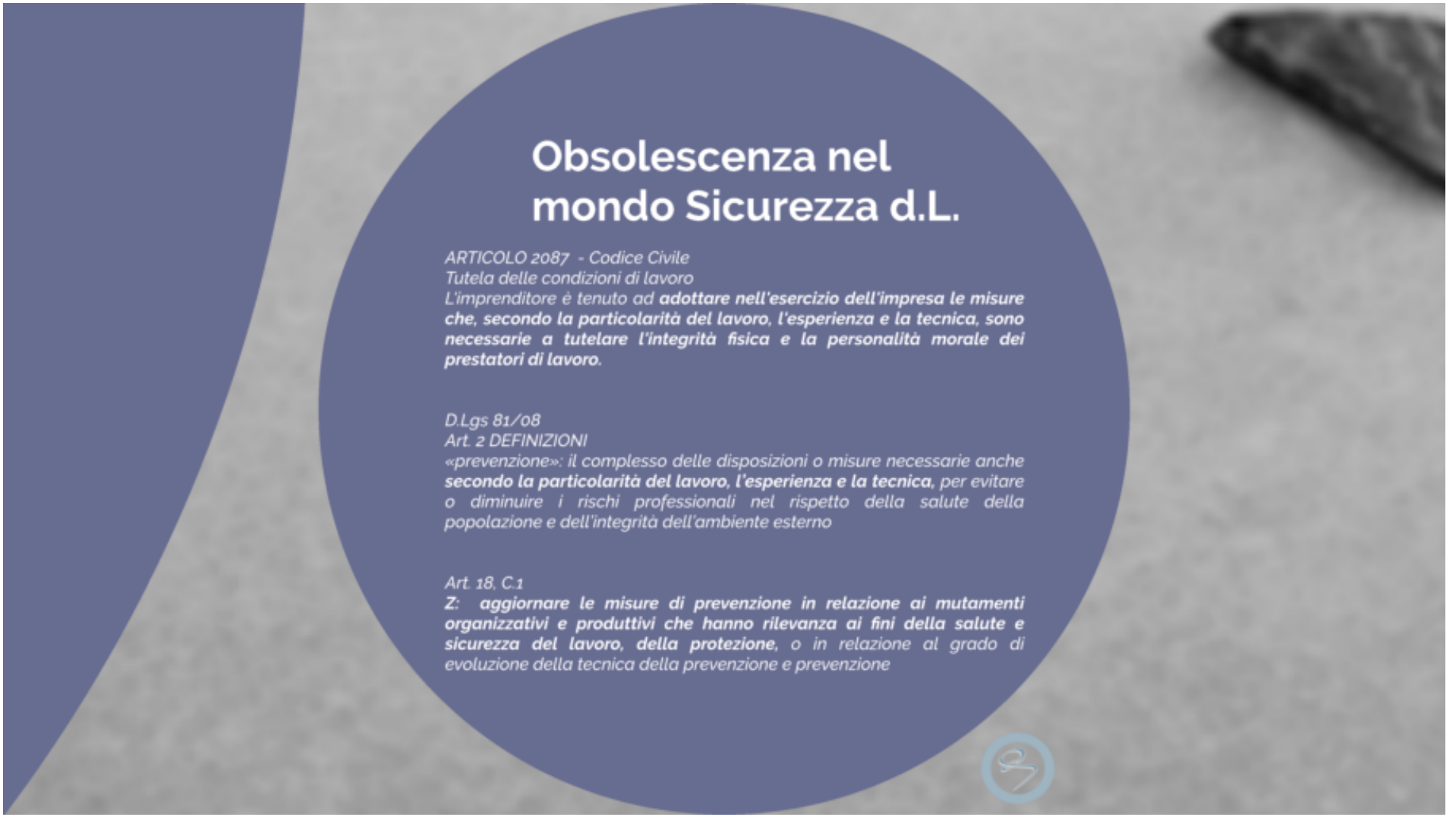
...

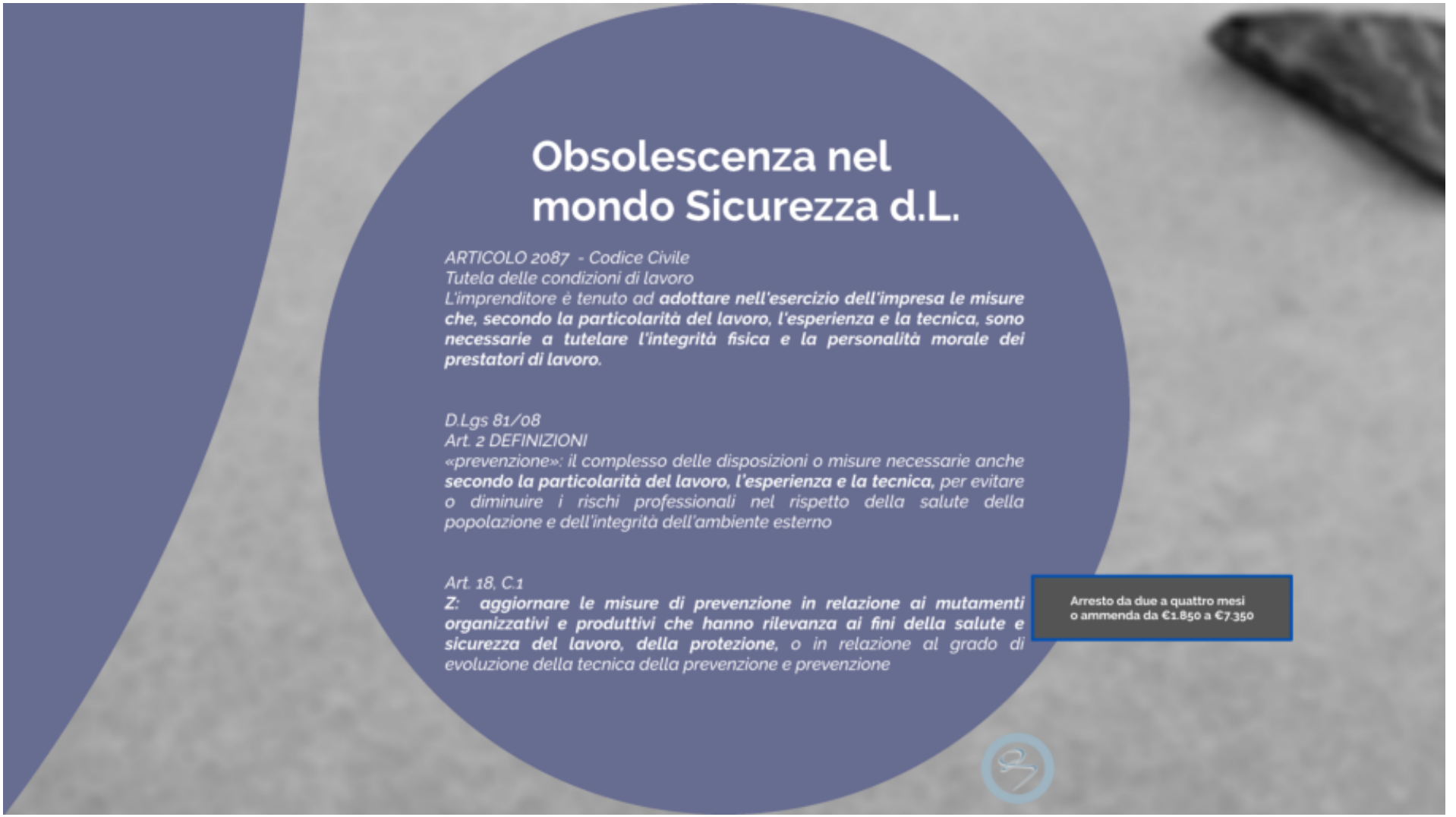
*3. entro il termine di 120 giorni dalla ricezione del presente provvedimento, ai fini del rispetto del **principio di responsabilizzazione** di cui all'articolo 24 del Regolamento, ad una rivisitazione complessiva delle iniziative di sicurezza adottate (cfr. par. 3.1 sulle **"Attività di vulnerability assessment"**),alcune delle quali, **per quanto conformi, in termini di stretto adempimento, alle prescrizioni di cui al par. 7, lett. A del provvedimento n. 548 del 2017, risultano comunque inficiate nella loro efficacia dalle gravi limitazioni tecniche intrinseche al sistema utilizzato** (CMS - Movable Type 4). L'eventuale inosservanza del presente ordine è soggetta alla sanzione amministrativa prevista dall'art. **83, par. 5, lett. e)** del Regolamento;*

sanzioni amministrativa fino a **20.000.000** EUR

4% del fatturato (anno prec.) se superiore


...
3. entro il termine di 120 giorni dalla ricezione del presente provvedimento, ai fini del rispetto del **principio di responsabilizzazione** di cui all'articolo 24 del Regolamento, ad una rivisitazione complessiva delle iniziative di sicurezza adottate (cfr. par. 3.1 sulle **"Attività di vulnerability assessment"**),alcune delle quali, **per quanto conformi, in termini di stretto adempimento, alle prescrizioni di cui al par. 7, lett. A del provvedimento n. 548 del 2017, risultano comunque inficiate nella loro efficacia dalle gravi limitazioni tecniche intrinseche al sistema utilizzato** (CMS - Movable Type 4). L'eventuale inosservanza del presente ordine è soggetta alla sanzione amministrativa prevista dall'art. **83, par. 5, lett. e)** del Regolamento;

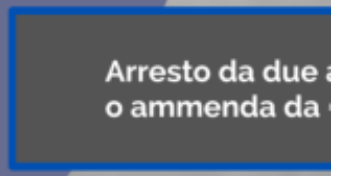

Obsolescenza nel mondo Sicurezza d.L.
ARTICOLO 2087 - Codice Civile
Tutela delle condizioni di lavoro
L'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro.
D.Lgs 81/08
Art. 2 DEFINIZIONI
«prevenzione»: il complesso delle disposizioni o misure necessarie anche secondo la particolarità del lavoro, l'esperienza e la tecnica, per evitare o diminuire i rischi professionali nel rispetto della salute della popolazione e dell'integrità dell'ambiente esterno
Art. 18, C.1
Z: aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, della protezione, o in relazione al grado di evoluzione della tecnica della prevenzione e prevenzione

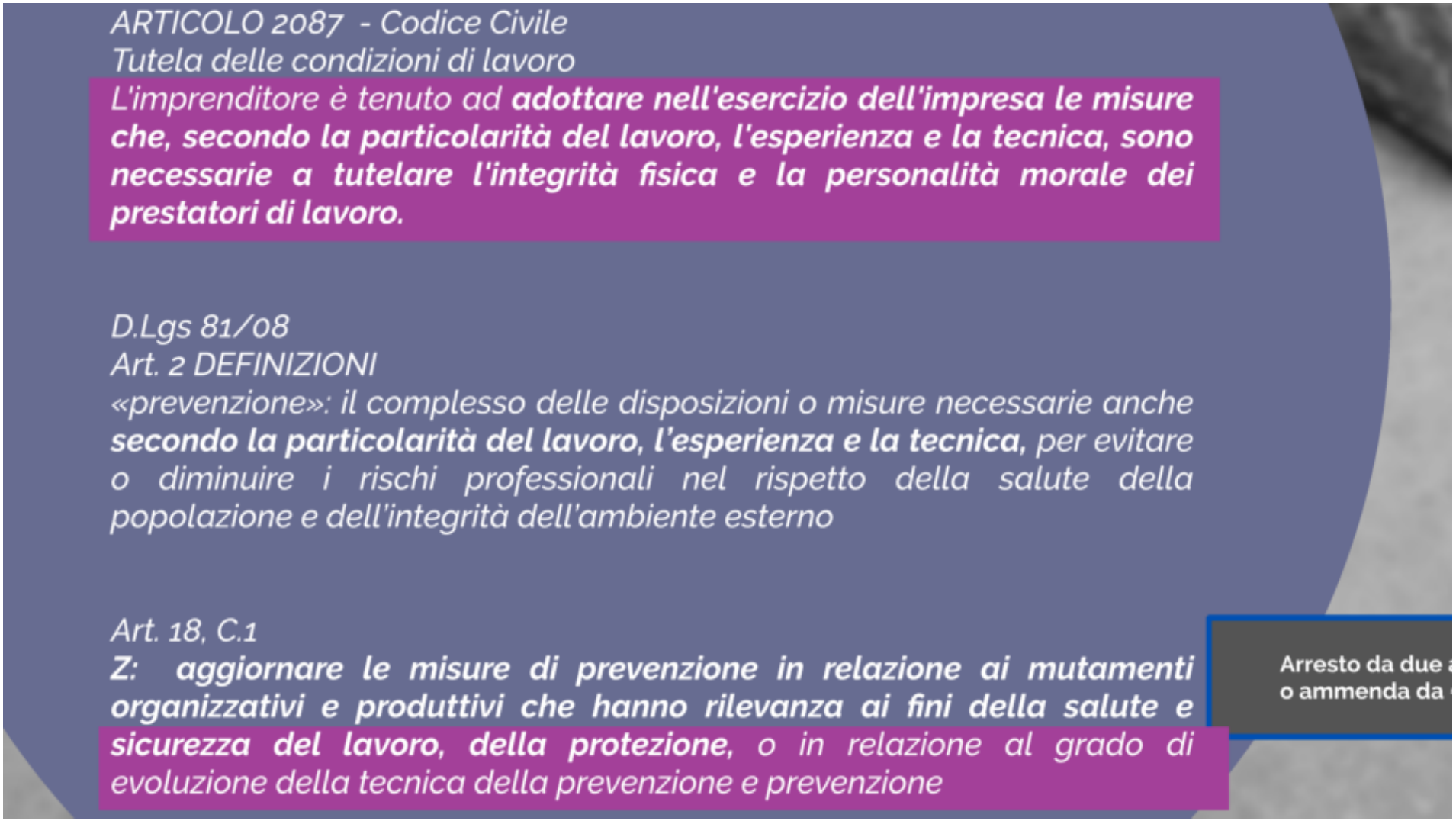

Obsolescenza nel mondo Sicurezza d.L.
ARTICOLO 2087 - Codice Civile
Tutela delle condizioni di lavoro
L'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro.
D.Lgs 81/08
Art. 2 DEFINIZIONI
«prevenzione»: il complesso delle disposizioni o misure necessarie anche secondo la particolarità del lavoro, l'esperienza e la tecnica, per evitare o diminuire i rischi professionali nel rispetto della salute della popolazione e dell'integrità dell'ambiente esterno
Art. 18, C.1
Z: aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, della protezione, o in relazione al grado di evoluzione della tecnica della prevenzione e prevenzione
Arresto da due a quattro mesi
o ammenda da €1.850 a €7.350

ARTICOLO 2087 - Codice Civile
Tutela delle condizioni di lavoro
L'imprenditore è tenuto ad ***adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro.***

D.Lgs 81/08
Art. 2 DEFINIZIONI
«prevenzione»: il complesso delle disposizioni o misure necessarie anche ***secondo la particolarità del lavoro, l'esperienza e la tecnica,*** *per evitare o diminuire i rischi professionali nel rispetto della salute della popolazione e dell'integrità dell'ambiente esterno*

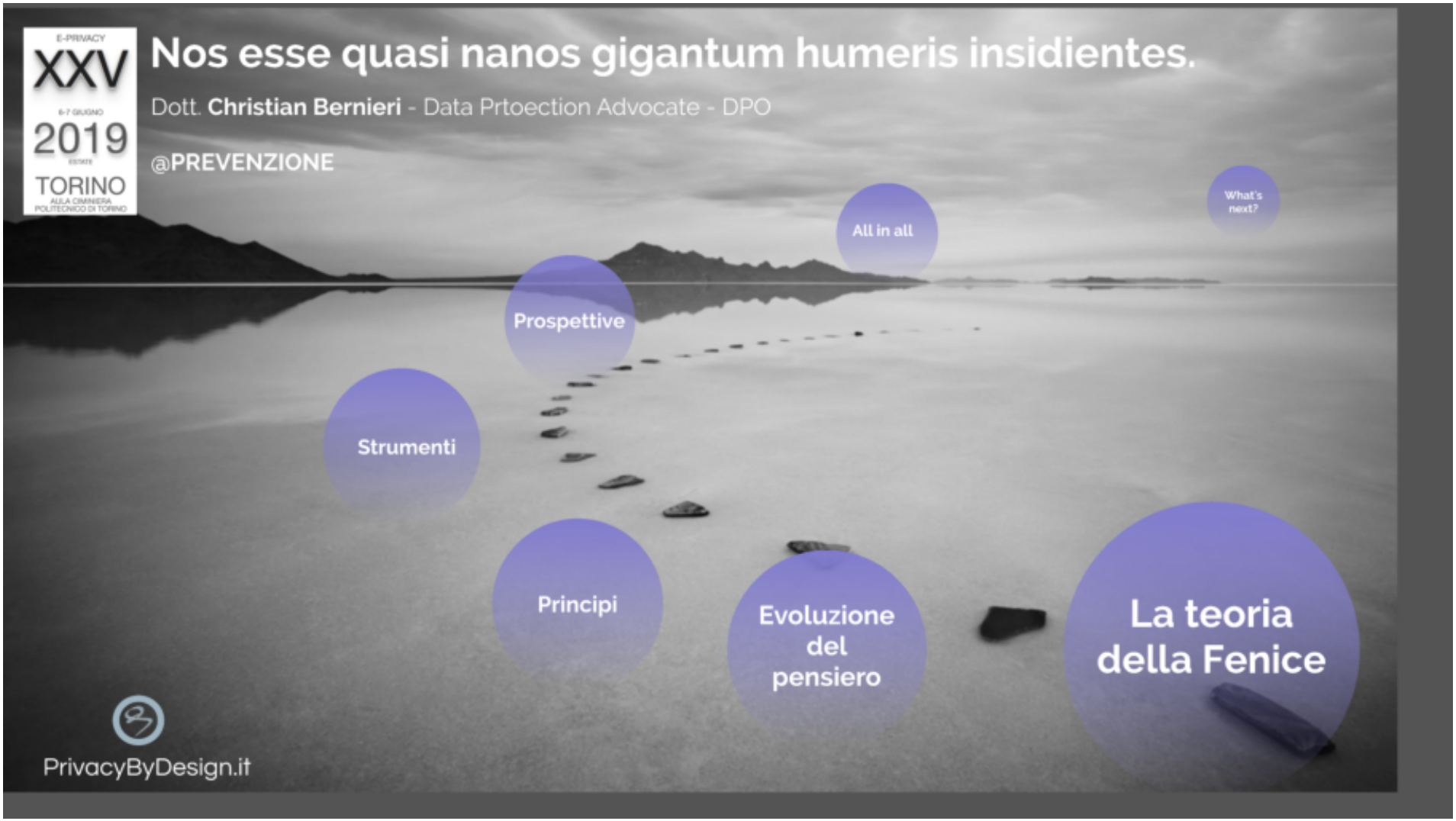
Art. 18, C.1
Z: aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, della protezione, *o in relazione al grado di evoluzione della tecnica della prevenzione e prevenzione*




ARTICOLO 2087 - Codice Civile
Tutela delle condizioni di lavoro
L'imprenditore è tenuto ad **adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro.**
D.Lgs 81/08
Art. 2 DEFINIZIONI
«prevenzione»: il complesso delle disposizioni o misure necessarie anche **secondo la particolarità del lavoro, l'esperienza e la tecnica**, per evitare o diminuire i rischi professionali nel rispetto della salute della popolazione e dell'integrità dell'ambiente esterno
Art. 18, C.1
Z: aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, della protezione, o in relazione al grado di evoluzione della tecnica della prevenzione e prevenzione
Arresto da due
o ammenda da


Responsabilità
GDPR: Articolo 82. Diritto al risarcimento e responsabilità
• Responsabilità (quasi) oggettiva
Art. 15 D.Lgs 196/03 - ABROGATO
• Responsabilità solidale
3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
4. ...ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno,


Responsabilità
GDPR: Articolo 82. Diritto al risarcimento e responsabilità
• Responsabilità (quasi) oggettiva
Art. 15 D.Lgs 196/03 - ABROGATO
• Responsabilità solidale
3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
4. ...ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno,


E-PRIVACY
XXV
6-7 GIUGNO
2019
EDIZIONE
TORINO
AULA CIMINIERA
POLITECNICO DI TORINO
Nos esse quasi nanos gigantum humeris insidientes.
Dott. Christian Bernieri - Data Prtoection Advocate - DPO
@PREVENZIONE
What's next?
All in all
Prospettive
Strumenti
Principi
Evoluzione del pensiero
La teoria della Fenice
PrivacyByDesign.it


Gli strumenti
Leader
ATTORI
Training
Near Miss
PbD
V.D.R.


Guardiamo oltre
Privacy by design e by default
Esempi
L'articolo 25 del GDPR
Nel mondo della **sicurezza**, si cerca di costruire macchine e organizzare processi **A PROVA DI IMBECILLE**.
Pensando a chi è più debole, mentalmente o fisicamente, si realizzano **sistemi sicuri in cui è impossibile farsi male**, nemmeno volendolo!
Nel mondo della **privacy**, si realizzano sistemi intrinsecamente sicuri, **integrando la prevenzione e la protezione in fase di progettazione** (P.b.Design), organizzandoli in modo che tutto possa funzionare senza alcuna scelta o impostazione dell'interessato, garantedogli **il massimo livello di protezione del dato come standard**. (P.b.Default)

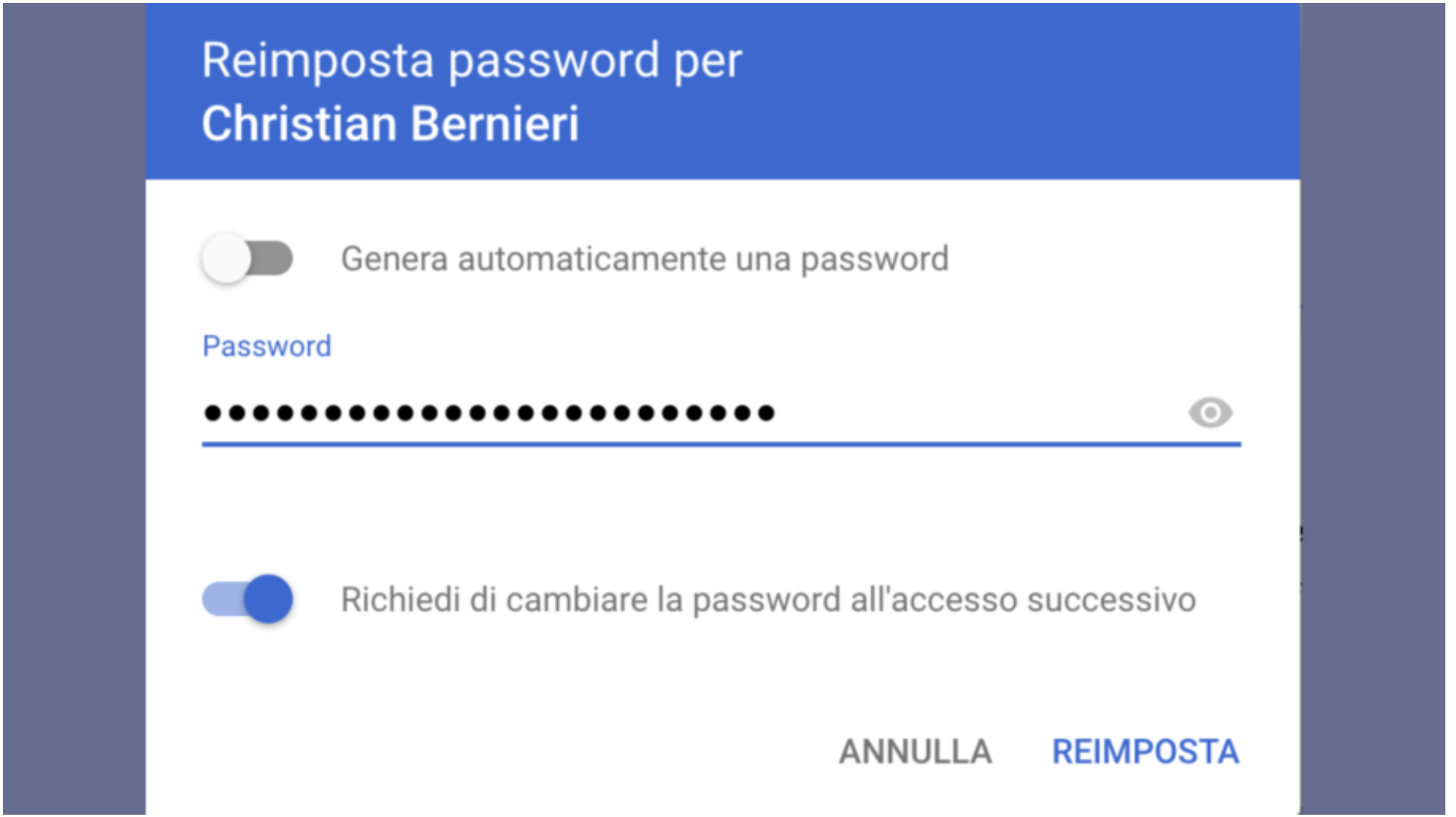
Guardando oltre...

- La privacy **a prova di imbecille**
- La privacy **a prova di errore**
- La privacy **a prova di distrazione**
- La privacy fin **dal primo giorno di lavoro**
- La privacy per il lavoratore **alloglotto**
- La privacy a prova di **decisione datoriale** (231)


Cos'è
e cosa NON E'
PbD

reddot design award
winner 2011


PAZIENTE
CON ICTUS


Reimposta password per
Christian Bernieri
Genera automaticamente una password
Password
Richiedi di cambiare la password all'accesso successivo
ANNULLA
REIMPOSTA

Formazione

Esempi

Nel mondo della **sicurezza**, la formazione è la chiave della prevenzione e prevede norme molto raffinate ed evolute.

- Informazione
- Formazione
- Addestramento
- Aggiornamento
- Formazione particolare per categorie speciali di rischio.

Nel mondo della **privacy**, la formazione è espressamente prevista dal GDPR ed è collegata al principio di **responsabilitzzazione** del Titolare.

I Garanti puntano molto **sull'alfabetizzazione** come strumento per bilanciare le anomalie applicative del GDPR.

La Formazione in azienda

Quadro di sintesi della formazione programmata

ARGOMENTO e DURATA	MODALITA'	DESTINATARI e PERIODICITA'
CORSO BASE – RUDIMENTI DI PROTEZIONE DEI DATI	Formazione in E-Learning oppure consegna di opuscolo informativo Senza verifica di apprendimento	Tutti i lavoratori neoassunti o trasferiti, a prescindere dalle mansioni affidate. Entro 2 mesi dall'ingresso in azienda. Senza aggiornamento periodico
CORSO COMPLETO PER LAVORATORI ADDETTI AL TRATTAMENTO **Minimo 2 ore**	Formazione in aula o videoconferenza. Consegna di materiale informativo Verifica di apprendimento mediante question time effettuata dal docente	Tutti i lavoratori individuati incaricati del trattamento, le cui mansioni prevedano il trattamento dati personali. Aggiornamento annuale
CORSO AVANZATO PER LAVORATORI ADDETTI ALLA SUPERVISIONE E VIGILANZA SUL TRATTAMENTO **Minimo 4 ore**	Formazione in aula o videoconferenza. Consegna di materiale informativo Verifica di apprendimento mediante question time effettuata dal docente	Tutti i lavoratori, che abbiano già svolto il corso completo, addetti alla supervisione del trattamento, vigilanza sull'attuazione delle misure di prevenzione e protezione. Aggiornamento triennale

PROGRAMMI DIDATTICI

CORSO COMPLETO – per tutti i lavoratori addetti al trattamento
DURATA IDEALE: 2 ore

MODULO TEORICO NORMATIVO

- Presentazione del corso, verifica delle competenze pregresse
- Normativa mondiale, europea, italiana, regionale
- I contenuti in dettaglio del regolamento UE 2016/679
- Interconnessione con altra normativa: codice penale, statuto dei lavoratori, 231, evoluzione della normativa e bozze di decreti in via di approvazione.
- I codici deontologici applicabili, l'etica professionale.
- Descrizione dei ruoli aziendali in materia di protezione dei dati, Titolare, autorizzati al trattamento, responsabile della protezione dei dati, responsabili esterni del trattamento
- Analisi dei trattamenti effettuati in azienda
- Concetti approfonditi di rischio relativo a DISPONIBILITA', RISERVATEZZA, INTEGRITA'
- Valutazione del rischio e tecnologie o procedure organizzative volte alla prevenzione e protezione
- Data Breach: modalità e tempistiche di segnalazione, doveri degli autorizzati e dei responsabili
- Protezione dei dati personali: misure organizzative, misure di prevenzione, misure di protezione, misure tecniche.

MODULO PRATICO OPERATIVO

- Compiti operativi degli autorizzati al trattamento
- La correttezza, il comportamento diligente del buon padre di famiglia.
- Finalità del trattamento e basi giuridiche di legittimazione del trattamento
- Modulistica aziendale per rendere l'informativa agli interessati
- Modalità di acquisizione del consenso
- Diritto degli interessati, modalità di esercizio e procedure per garantire esercizio dei diritti
- Gestione delle richieste di accesso ai dati, dei reclami, dell'opposizione al trattamento
- Misure di prevenzione e protezione sia per i dati digitali sia per i dati cartacei
- Utilizzo delle infrastrutture e dei sistemi informativi
- Approfondimento sulla gestione dei dati con strumenti informatici, in particolare: Email, Web, Spreadsheet e data management, Archivi, File Server.
- Approfondimento sulla gestione delle credenziali di autenticazione: password, chiavi di autenticazione, profili di autorizzazione.
- Applicazioni, Gestionali, Dati e metadati (i dati invisibili), Data transfer (dispositivi esterni, invio file, memorie, ecc), Cloud computing, Sistemi di comunicazione, dispositivi mobili.
- Istruzioni operative di dettaglio
- Come riconoscere se qualcosa non va, Come riconoscere un Data Breach, come gestire intrusioni informatiche
- Consegna dei materiali informativi
- Question time - soluzione di problemi e temi proposti dall'autorizzato al trattamento.
- Verifica di apprendimento

CARATTERISTICHE GENERALI DI OGNI CORSO DI FORMAZION
ORGANIZZAZIONE DELLA FORMAZIONE

Per ciascun corso si dovrà prevedere:
a) soggetto organizzatore del corso, preferibilmente con l'intervento del DPO;
b) un responsabile del progetto formativo;
c) i nominativi dei docenti;
d) un numero massimo di partecipanti ad ogni corso pari a 30 unità;
e) il registro di presenza dei partecipanti;
f) l'obbligo di frequenza del 90% delle ore di formazione previste;
g) la declinazione dei contenuti tenendo presenti le differenze di genere, di età, di prov
nonché i rischi connessi alla specifica tipologia contrattuale attraverso cui viene resa la p
lavoro.

Ogni corso sarà formalmente documentato e darà luogo all'emissione di attestati per il s

Il corso BASE è strutturato e veicolato per mezzo di una piattaforma di E-Learning dedica
consiste nella dazione di una serie di materiali informativi.

L'ufficio risorse umane effettua il monitoraggio dell'effettuazione e della regolare conclu

Quadro di sintesi della formazione programmata

ARGOMENTO e DURATA	MODALITA'	DESTINATARI e PERIODICITA'
CORSO BASE – RUDIMENTI DI PROTEZIONE DEI DATI	Formazione in E-Learning oppure consegna di opuscolo informativo Senza verifica di apprendimento	Tutti i lavoratori neoassunti o trasferiti, a prescindere dalle mansioni affidate. Entro 2 mesi dall'ingresso in azienda. Senza aggiornamento periodico
CORSO COMPLETO PER LAVORATORI ADDETTI AL TRATTAMENTO **Minimo 2 ore**	Formazione in aula o videoconferenza. Consegna di materiale informativo Verifica di apprendimento mediante question time effettuata dal docente	Tutti i lavoratori individuati incaricati del trattamento, le cui mansioni prevedano il trattamento dati personali. Aggiornamento annuale
CORSO AVANZATO PER LAVORATORI ADDETTI ALLA SUPERVISIONE E VIGILANZA SUL TRATTAMENTO **Minimo 4 ore**	Formazione in aula o videoconferenza. Consegna di materiale informativo Verifica di apprendimento mediante question time effettuata dal docente	Tutti i lavoratori, che abbiano già svolto il corso completo, addetti alla supervisione del trattamento, vigilanza sull'attuazione delle misure di prevenzione e protezione. Aggiornamento triennale

CORSO COMPLETO – p
DURATA IDEALE: 2 ore

MODULO TEORICO NC

- Presentazione del corso,
- Normativa mondiale, eu
- I contenuti in dettaglio d
- Interconnessione con al normativa e bozze di de
- I codici deontologici ap
- Descrizione dei ruoli azie responsabile della prote
- Analisi dei trattamenti el
- Concetti approfonditi di
- Valutazione del rischio e
- Data Breach: modalità
- Protezione dei dati pers misure tecniche.

MODULO PRATICO OP

- Compiti operativi degli
- La correttezza, il compo
- Finalità del trattamento
- Modulistica aziendale p
- Modalità di acquisizione
- Diritto degli interessati, n
- Gestione delle richieste
- Misure di prevenzione e
- Utilizzo delle infrastruttur
- Approfondimento sulla Spreadsheet e data ma
- Approfondimento sulla autenticazione, profili di
- Applicazioni, Gestionali, memorie, ecc). Cloud c
- Istruzioni operative di de

DESTINATARI e PERIODICITA'
Tutti i lavoratori neoassunti o trasferiti, a prescindere dalle mansioni affidate. Entro 2 mesi dall'ingresso in azienda. Senza aggiornamento periodico
Tutti i lavoratori individuati incaricati del trattamento, le cui mansioni prevedano il trattamento dati personali. Aggiornamento annuale
Tutti i lavoratori, che abbiano già svolto il corso completo, addetti alla supervisione del trattamento, vigilanza sull'attuazione delle misure di prevenzione e protezione. Aggiornamento triennale

PROGRAMMI DIDATTICI

CORSO COMPLETO – per tutti i lavoratori addetti al trattamento
DURATA IDEALE: 2 ore

MODULO TEORICO NORMATIVO

- Presentazione del corso, verifica delle competenze pregresse
- Normativa mondiale, europea, italiana, regionale
- I contenuti in dettaglio del regolamento UE 2016/679
- Interconnessione con altra normativa: codice penale, statuto dei lavoratori, 231, evoluzione della normativa e bozze di decreti in via di approvazione.
- I codici deontologici applicabili, l'etica professionale,
- Descrizione dei ruoli aziendali in materia di protezione dei dati, titolare, autorizzati al trattamento, responsabile della protezione dei dati, responsabili esterni del trattamento
- Analisi dei trattamenti effettuati in azienda
- Concetti approfonditi di rischio relativo a DISPONIBILITA', RISERVATEZZA, INTEGRITA'
- Valutazione del rischio e tecnologie o procedure organizzative volte alla prevenzione e protezione
- Data Breach: modalità e tempistiche di segnalazione, doveri degli autorizzati e dei responsabili
- Protezione dei dati personali: misure organizzative, misure di prevenzione, misure di protezione, misure tecniche.

MODULO PRATICO OPERATIVO

- Compiti operativi degli autorizzati al trattamento
- La correttezza, il comportamento diligente del buon padre di famiglia.
- Finalità del trattamento e basi giuridiche di legittimazione del trattamento
- Modulistica aziendale per rendere l'informativa agli interessati
- Modalità di acquisizione del consenso
- Diritto degli interessati, modalità di esercizio e procedure per garantire esercizio dei diritti
- Gestione delle richieste di accesso ai dati, dei reclami, dell'opposizione al trattamento
- Misure di prevenzione e protezione sia per i dati digitali sia per i dati cartacei
- Utilizzo delle infrastrutture e dei sistemi informativi
- Approfondimento sulla gestione dei dati con strumenti informatici, in particolare: Email, Web, Spreadsheet e data management, Archivi, File Server,
- Approfondimento sulla gestione delle credenziali di autenticazione: password, chiavi di autenticazione, profili di autorizzazione,
- Applicazioni, Gestionali, Dati e metadati (i dati invisibili), Data transfer (dispositivi esterni, invio file, memorie, ecc), Cloud computing, Sistemi di comunicazione, dispositivi mobili.
- Istruzioni operative di dettaglio
- Come riconoscere se qualcosa non va. Come riconoscere un Data Breach, come gestire intrusioni informatiche
- Consegna dei materiali informativi
- Question time - soluzione di problemi e temi proposti dall'autorizzato al trattamento.
- Verifica di apprendimento

CARATTERISTICHE
ORGA

Per ciascun corso si dovrà prevedere:
a) soggetto organizzatore del corso, pr
b) un responsabile del progetto formati
c) i nominativi dei docenti;
d) un numero massimo di partecipanti
e) il registro di presenza dei partecipant
f) l'obbligo di frequenza del 90% delle o
g) la declinazione dei contenuti tenend
nonché i rischi connessi alla specifica ti
lavoro.

Ogni corso sarà formalmente documen

Il corso BASE è strutturato e veicolato pe
consiste nella dazione di una serie di m

L'ufficio risorse umane effettua il monito

CARATTERISTICHE GENERALI DI OGNI CORSO DI FORMAZIONE
ORGANIZZAZIONE DELLA FORMAZIONE

Per ciascun corso si dovrà prevedere:
a) soggetto organizzatore del corso, preferibilmente con l'intervento del DPO;
b) un responsabile del progetto formativo;
c) i nominativi dei docenti;
d) un numero massimo di partecipanti ad ogni corso pari a 30 unità;
e) il registro di presenza dei partecipanti;
f) l'obbligo di frequenza del 90% delle ore di formazione previste;
g) la declinazione dei contenuti tenendo presenti: le differenze di genere, di età, di provenienza e lingua, nonché i rischi connessi alla specifica tipologia contrattuale attraverso cui viene resa la prestazione di lavoro.

Ogni corso sarà formalmente documentato e darà luogo all'emissione di attestati per il singolo lavoratore.

Il corso BASE è strutturato e veicolato per mezzo di una piattaforma di E-Learning dedicata o, in alternativa, consiste nella dazione di una serie di materiali informativi.

L'ufficio risorse umane effettua il monitoraggio dell'effettuazione e della regolare conclusione dei corsi.

Leader

Datore di lavoro - Titolare del trattamento

Nel mondo della **sicurezza**, si individuano sempre le **PERSONE** con **il potere decisionale e di spesa.**
Queste sono chiamate alla realizzazione di tutti gli adempimenti e hanno limitati poteri di delega.
E' un **ruolo DI FATTO**, che può prescindere da investitura o ufficialità (art 299 D.Lgs 81/08).

Nel mondo della **privacy**, il titolare è generalmente l'ente nel suo complesso, ed è colui che determ**ina le finalità e i mezzi del trattamento.**

Ci sono ampi **margini per definire i ruoli tra differenti soggetti.**


Attori interni
Lo strumento del GDPR
I SOGGETTI ATTORI
Datore di lavoro - Titolare del trattamento
Nel mondo della **sicurezza**, i ruoli sono ben definiti dalla legge e partecipano con funzioni differenti agli obblighi di prevenzione
Nel mondo della **privacy**, il GDPR lascia una grande liberà organizzativa e basa tutto sull'organizzazione realizzata dla titolare e dal suo governo del processo produttivo.


Gli attori interni
Sicurezza
Datore di Lavoro
Dirigente
Preposto
Lavoratore
Privacy
Titolare
non definito?
non definito?
non definito?


D.Lgs 196/03 (Mod D.Lgs 101/18)
Art. 2-quaterdecies
(Attribuzione di funzioni e compiti a soggetti designati)
1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilita' e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.
2. Il titolare o il responsabile del trattamento individuano le modalita' piu' opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorita' diretta.


Gli attori esterni
Sicurezza
Azienda
Fornitori-Appaltatori
Prestatori d'opera
Committenti
Privacy
Titolare
Responsabili del trattamento
Incaricati - Responsabili d. t.
Co-Titolari - Titolari

GUIDA ALL'INDIVIDUAZIONE DEL CORRETTO RUOLO TRA
TITOLARE (Data Controller)
COTITOLARE (Joint Data Controller)
RESPONSABILE DEL TRATTAMENTO (Data Processor)

CRITERI DEDUTTIVI - DESCRITTIVI

Se eserciti il controllo globale sulle finalità e sulle modalità del trattamento dei dati personali, ad esempio, decidi quali dati elaborare e perché: sei un controllore.

Se non hai uno scopo tuo proprio per elaborare i dati e agisci solo su istruzioni di un cliente, è probabile che tu sia un responsabile del trattamento, anche se prendi alcune decisioni tecniche su come elaborare i dati.

CRITERI INDUTTIVI

Siamo un Titolare del trattamento...

Abbiamo deciso di raccogliere o trattare i dati personali?
Abbiamo deciso quale doveva essere lo scopo o il risultato dell'elaborazione.
Abbiamo deciso quali dati personali vadano raccolti?
Abbiamo deciso chi debbano essere i soggetti di cui raccogliamo i dati?
Abbiamo un vantaggio commerciale o un ritorno dal trattamento (escluso l'eventuale pagamento da terzi per il servizio di elaborazione)
Trattiamo i dati in funzione di un contratto tra noi e l'interessato?
Gli interessati sono nostri lavoratori?
Prendiamo decisioni in merito alle persone interessate come parte o come risultato dell'elaborazione.
Formuliamo giudizi professionali nel trattamento dei dati personali.
Abbiamo un rapporto diretto con gli interessati?
Abbiamo completa autonomia su come vengono trattati i dati personali.
Abbiamo nominato responsabili del trattamento per elaborare i dati personali per nostro conto.

Siamo un co-titolare...

Abbiamo un obiettivo comune con gli altri per quanto riguarda il trattamento?
Trattiamo i dati per le stesse finalità comuni ad un altro titolare?
Utilizziamo lo stesso database per il trattamento in comune con un altro titolare?
Abbiamo progettato il trattamento assieme ad un altro titolare?
Abbiamo regole condivise con un altro titolare per il trattamento?

Siamo un responsabile del trattamento ...

Seguiamo le istruzioni di qualcun altro riguardo al trattamento dei dati personali.
Ci sono stati consegnati i dati personali da un cliente o una parte terza, o ci è stato detto quali dati raccogliere?
Non abbiamo deciso noi di raccogliere i dati presso gli interessati?
Non abbiamo deciso noi quali dati raccogliere dagli interessati.
Non abbiamo deciso noi le basi di legittimità del trattamento.
Non abbiamo deciso le finalità del trattamento.
Non abbiamo deciso se
Non decidiamo se divulgare i dati o a chi comunicarli.
Non abbiamo deciso per quanto tempo conservare i dati.
Potremmo prendere alcune decisioni su come vengono elaborati i dati, ma implementare queste decisioni sulla base di un contratto con qualcun altro.
Non siamo interessati al risultato finale dell'elaborazione.

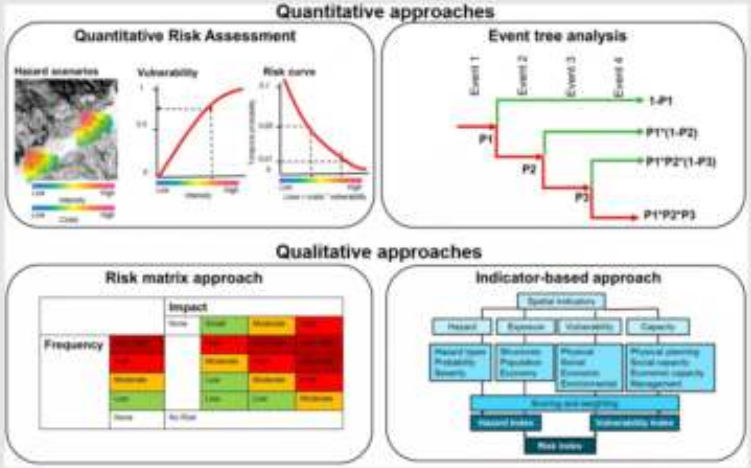
PER MAGGIORI DETTAGLI SI VEDA IL DOCUMENTO DI CHIARIMENTO DEL GARANTE ITALIANO A QUESTO INDIRIZZO:
DocWeb 9080970 - https://www.garanteprivacy.it/garante/doc.jsp?ID=9080970

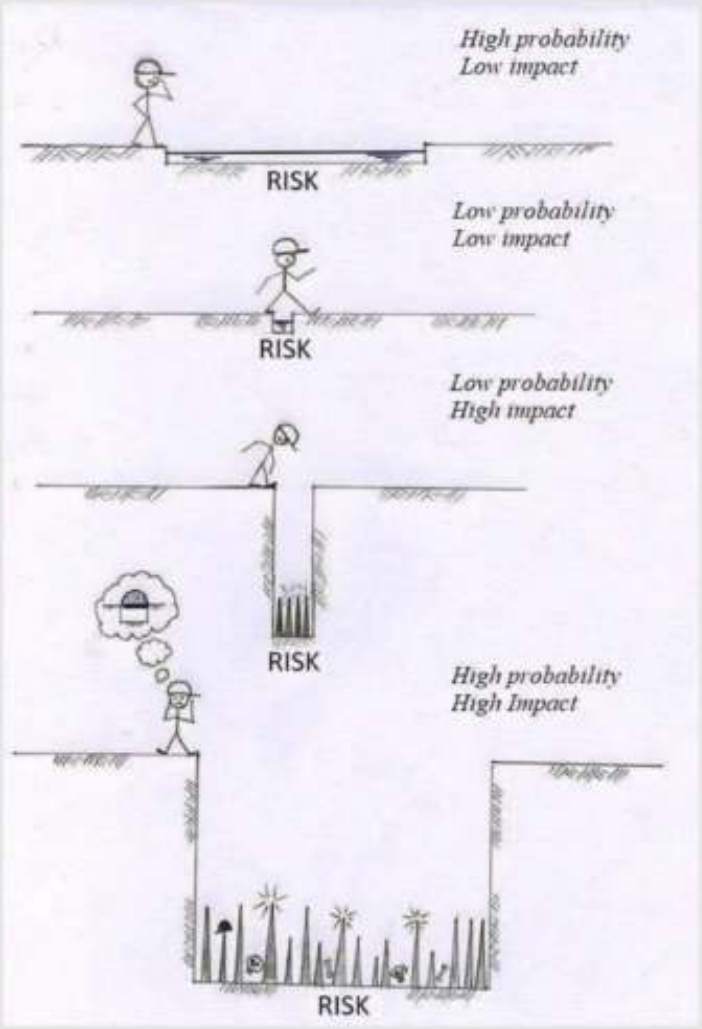

Near Miss
Come trasformare i problemi in opportunità
SICUREZZA
strumento consolidato per riportare gli incidenti senza conseguenze
al fine di attivare misure per **prevenire identici incidenti in futuro**
PRIVACY
nuovo strumento ancora da capire, utilizzare e raffinare:
REGISTRO DEI TRATTAMENTI

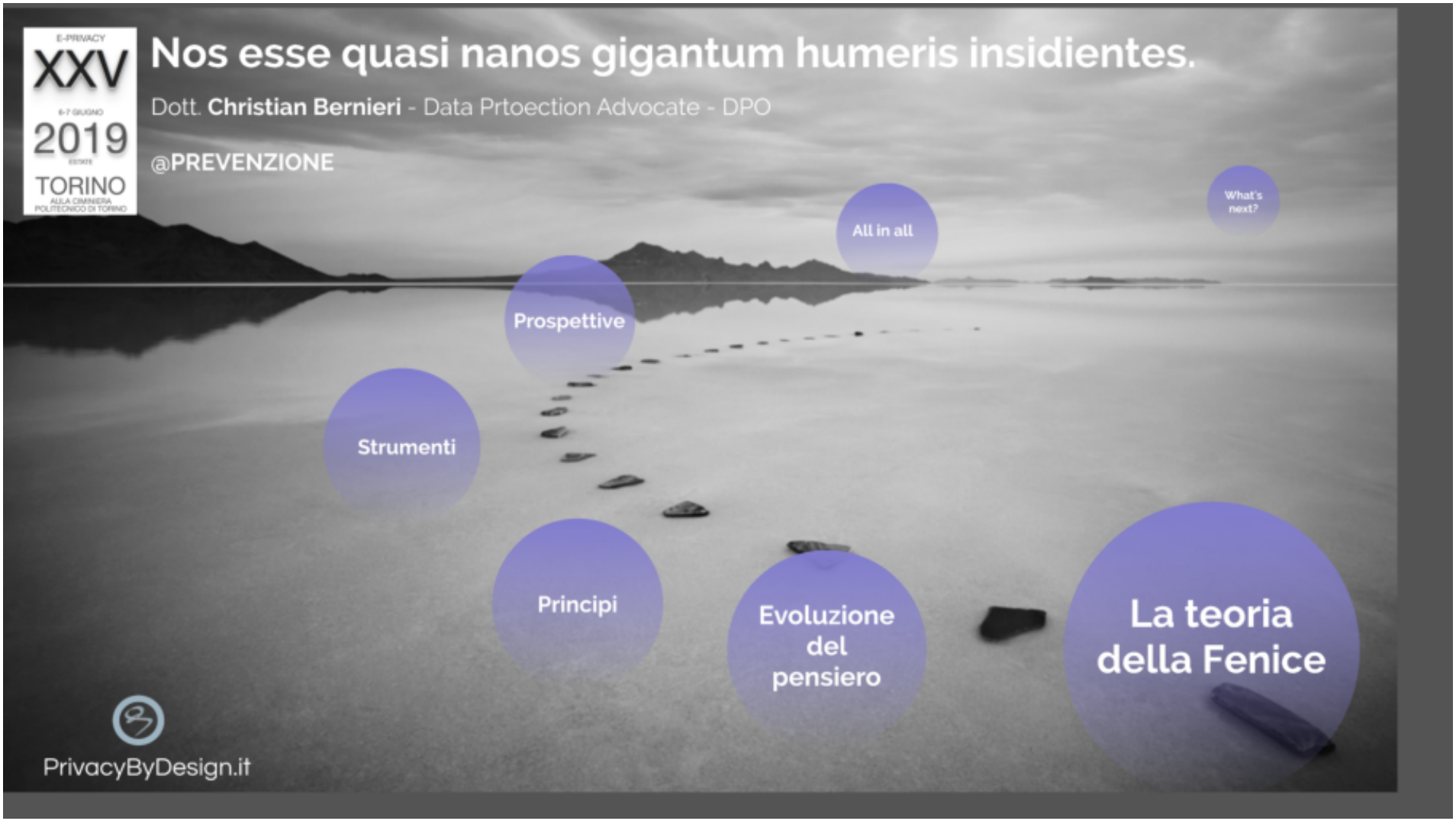

Valutazione del Rischio
Misurare - Confrontare - Ponderare
SICUREZZA
VDR - Valutazione dei Rischi
DUVRI - Valutazione rischi Interferenziali
Valutazione Qualitativa
Valutazione Quantitativa
PRIVACY
Registro dei trattamenti Titolare
Registro dei trattamenti Responsabile
DPIA - Data Protection Impact Assessment

Probabilità dell'evento
Gravità del danno atteso

PxG=Rischio






E-PRIVACY
XXV
6-7 GIUGNO
2019
TORINO
AULA CIMINIERA
POLITECNICO DI TORINO
Nos esse quasi nanos gigantum humeris insidientes.
Dott. Christian Bernieri - Data Prtoection Advocate - DPO
@PREVENZIONE
What's next?
All in all
Prospettive
Strumenti
Principi
Evoluzione del pensiero
La teoria della Fenice
PrivacyByDesign.it


QUALIFICA
MISURA
COMPETIZIONE
VERIFICA
Margini di miglioramento
STANDARD
DOVERI
HI-RISKS


Doveri dei lavoratori
Nella Sicurezza sono espressamente previsti i DOVERI DEI LAVORATORI che permettono di attuare le misure previste dal datore di lavoro.
Nella Privacy non ci sono misure prescrittive o di indicazione destinate ai lavoratori o agli autorizzati al trattamento.
Si fa solo riferimento alla autorità del titolare o alla diretta autorità del titolare.


Garantire l'attuazione
Nella sicurezza del lavoro è ben strutturato il meccanismo che garantisce al datore di lavoro l'applicazione delle norme da parte dei lavoratori (PREPOSTI)
Nella Privacy, questo meccanismo di verifica e garanzia di attuazione è completamente assente.
Viene citato solo il dovere del Responsabile del trattamento di segnalare attività contrarie al GDPR.


MISURA DEI RISULTATI
La sicurezza oggi si fonda sul monitoraggio dei risultati, L'analisi dei dati collettivi, raffrontati con quelli della specifica azienda, permette di comprendere l'effettivo andamento della prevenzione..
Per la privacy mancano i dati: oggi i dati sono pochi solo le autorità garanti pubblicano alcune statistiche sulla loro operatività.


Qualifica dei fornitori
• La sicurezza del lavoro fa largo uso della qualifica tecnico professionale.
• Le aziende scelgono sulla base di indicatori che misurano la sicurezza
• I contratti agganciano la loro validità all'esito di audit sulla sicurezza
• Le violazioni sono causa di risoluzione espressa
La Privacy prevede le certificazioni e le aziende iniziano a qualificare i fornitori ma siamo agli albori rispetto allo scenario già delineato per la prevenzione.


Competizione
Le aziende competono sulla sicurezza.
Un tempo questa era un'area dove cercare margine ed utile economico mediante risparmio.
Oggi è elemento distintivo per accedere a bandi o gare con precisi vincoli.
Committenti nazionali prediligono aziende locali poichè gli adempimenti sono omogenei, confrontabili e verificabili.
Per la Privacy, i fornitori sono spesso stranieri e le certificazioni avranno un ruolo importante per garantire omogeneità, confrontabilità e verificabilità.

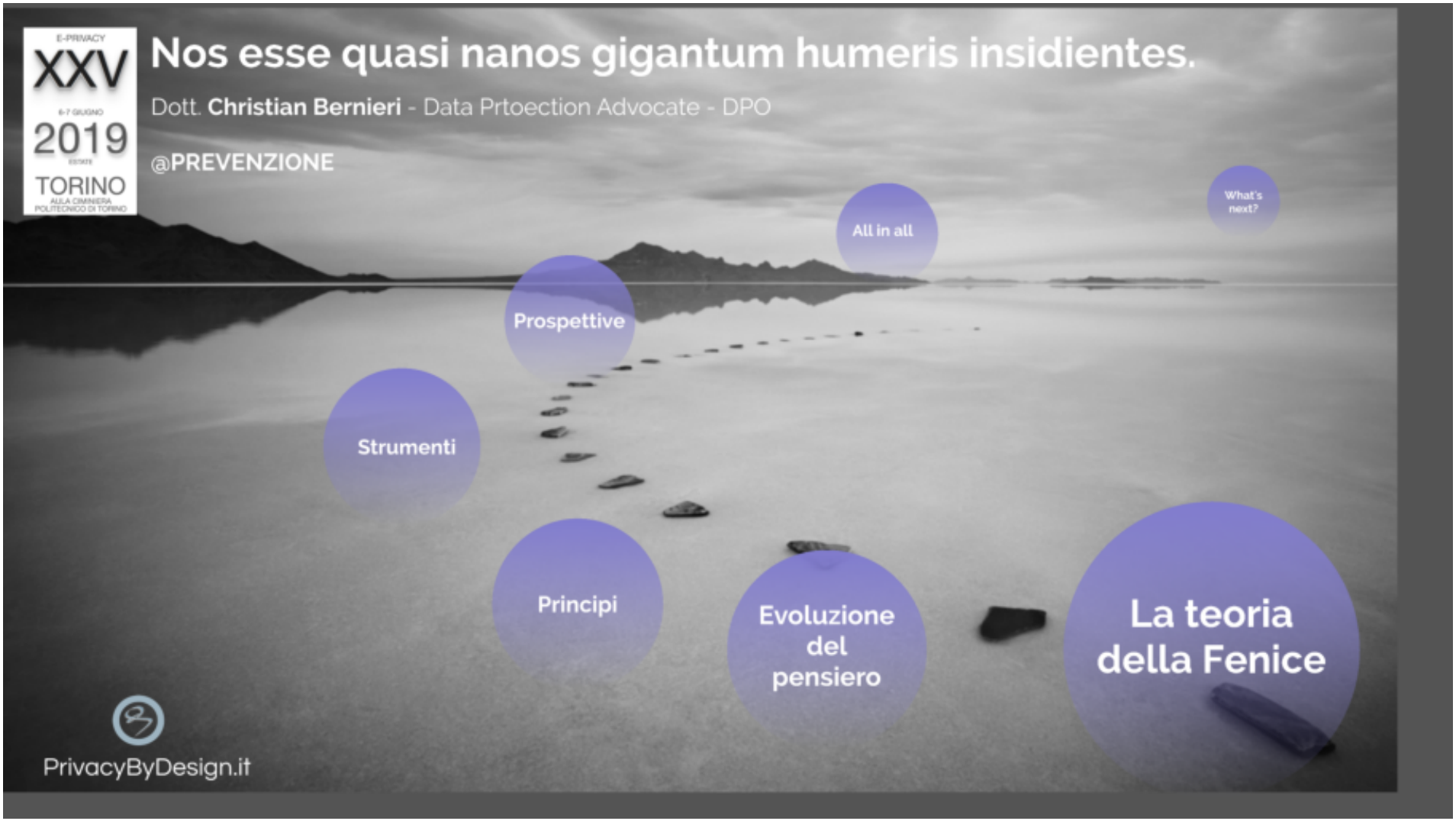

Standardizzazione
Recente tendenza della sicurezza è utilizzare dei service specializzati, dei Portali e piattaforme di qualifica, asettici, imparziali, e con controlli formali maniacali, adottando livelli di qualifica molto superiori a quelli previsti dalla norma di legge.
Era una tendenza presso grandi aziende e multinazionali ad alto rischio. Si sta diffondendo anche ad aziende piccole o a rischio molto più basso.


Hi-Risks
L'uso di particolari attrezzature o l'esposizione a particolari rischi richiede misure specificamente previste:
• Formazione minima di X ore
• Addestramento come attività aggiuntiva alla formazione
• Esperienza minima di X anni
• Riunioni di coordinamento da realizzare caso per caso
• Istituzione di preposti alle attività con compito di vigilanza continuativa
• Permessi di lavoro
• Iscrizione in appositi registri di soggetti abilitati.


Hi-Risks
L'uso di particolari attrezzature o l'esposizione a particolari rischi richiede misure specificamente previste:
• Formazione minima di X ore
• Addestramento come attività aggiuntiva alla formazione
• Esperienza minima di X anni
• Riunioni di coordinamento da realizzare caso per caso
• Istituzione di preposti alle attività con compito di vigilanza continuativa
• Permessi di lavoro
• Iscrizione in appositi registri di soggetti abilitati.

In Materia di Protezione dei Dati, sono già previsti **adempimenti particolari per particolari tipologie di trattamenti** (Elenco trattamenti soggetti a DPIA - Registro - DPIA - Consultazione Preventiva).

Questi strumenti, nel tempo, sono stati fortemente potenziati nel mondo della sicurezza del lavoro

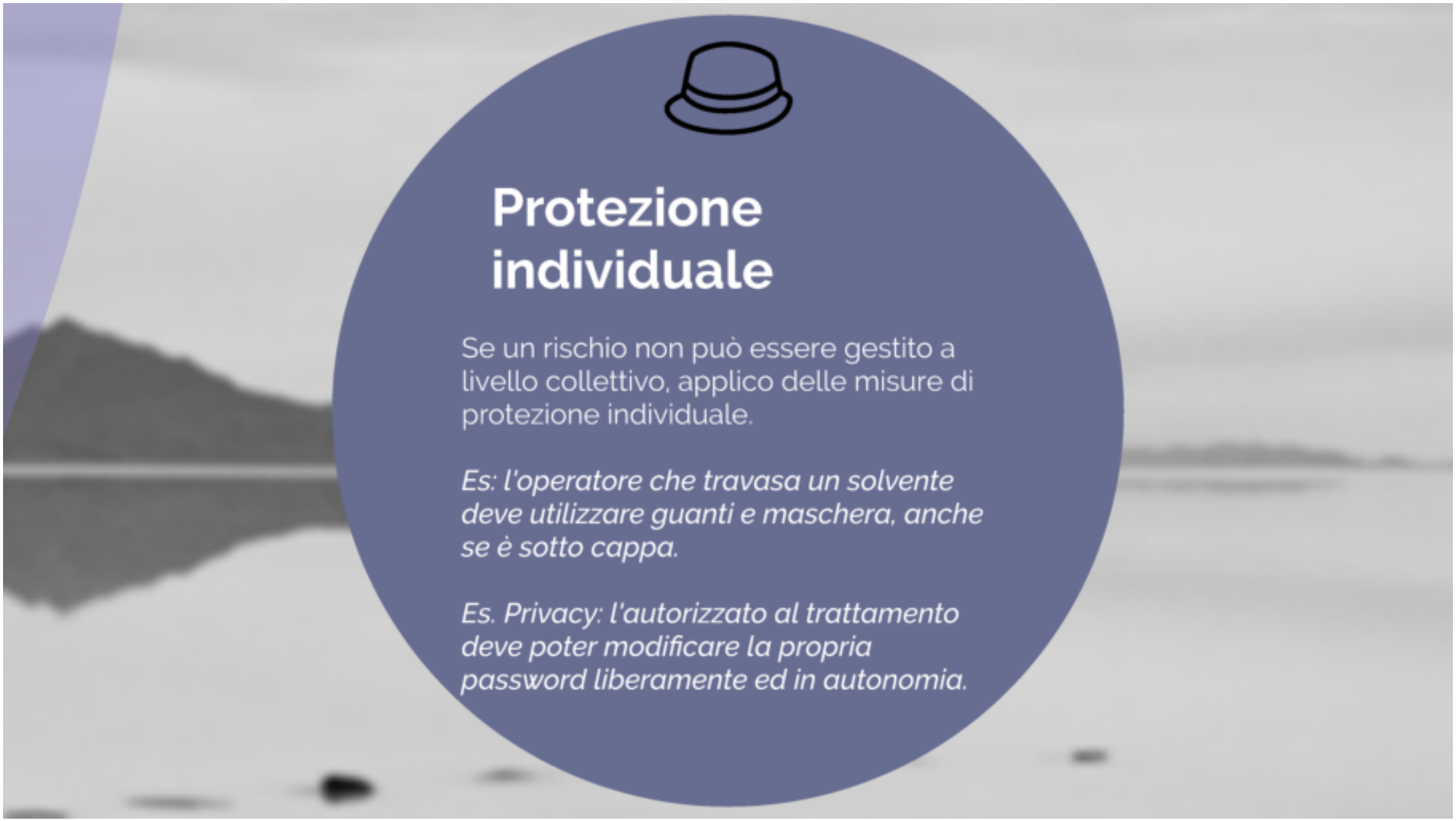

E-PRIVACY
XXV
6-7 GIUGNO
2019
EDIZIONE
TORINO
AULA CIMINIERA
POLITECNICO DI TORINO
Nos esse quasi nanos gigantum humeris insidientes.
Dott. Christian Bernieri - Data Prtoection Advocate - DPO
@PREVENZIONE
What's next?
All in all
Prospettive
Strumenti
Principi
Evoluzione del pensiero
La teoria della Fenice
PrivacyByDesign.it


I cardini della sicurezza del lavoro
sono ben collaudati e sono presenti anche nella normativa in materia di protezione dei dati personali.
Evita
1
Sostituisci
2
Proteggi tutti
3
Proteggi l'individuo
4
Misure reattive
5

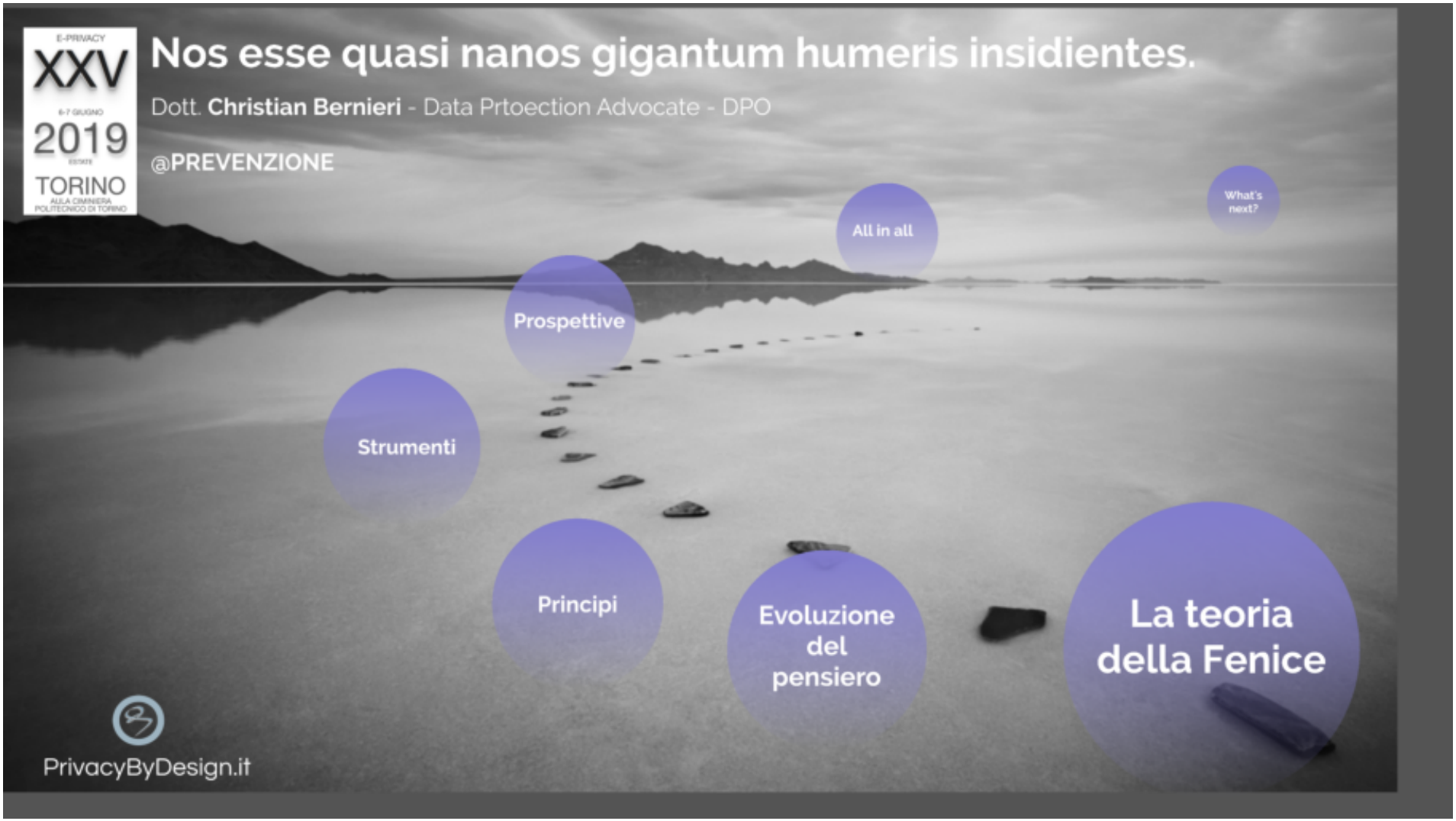

EVITA
Se possibile, evitare i rischi.
Es. Fare un lavoro a terra anzichè in quota.
Es. Privacy:
Non trattare dati personali per una finalità che puoi raggiungere anche senza.
PRINCIPIO DI MINIMIZZAZIONE.
GDPR Art 5.1.c
I dati personali sono: adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);


Sostituisci
Sostituisci ciò che è più pericoloso con cio che lo è meno.
Es. Sostituisco le vernici a Solvente con le vernici ad acqua, anche se costano di più.
Es. Privacy: utilizzo un PIN o RFID anzichè un lettore biometrico di impronte per accedere ad aree riservate.


Protezione collettiva
Se un rischio permane, attuo una protezione collettiva a beneficio di chiunque operi nell'area.
Es: travaso un solvente... sotto una cappa aspirante
Es. Privacy: sulle connesisoni internet applico un firewall e uso una blacklist di domini e siti.


Protezione individuale
Se un rischio non può essere gestito a livello collettivo, applico delle misure di protezione individuale.
Es: l'operatore che travasa un solvente deve utilizzare guanti e maschera, anche se è sotto cappa.
Es. Privacy: l'autorizzato al trattamento deve poter modificare la propria password liberamente ed in autonomia.


Misure Reattive
Se un rischio è nell'orizzonte degli eventi e ti aspetti che possa capitare...
Preparati al peggio con dei piani di risposta e reazione.
Es. Sicurezza:
PIANI DI GESTIONE EMERGENZE
PRONTO INTERVENTO.
Es. Privacy:
Data Breach Response Plan
Business Continuity
Disaster Recovery


E-PRIVACY
XXV
6-7 GIUGNO
2019
EDIZIONE
TORINO
AULA CIMINIERA
POLITECNICO DI TORINO
Nos esse quasi nanos gigantum humeris insidientes.
Dott. Christian Bernieri - Data Prtoection Advocate - DPO
@PREVENZIONE
What's next?
All in all
Prospettive
Strumenti
Principi
Evoluzione del pensiero
La teoria della Fenice
PrivacyByDesign.it


Cosa ci riserva il futuro?
Sicurezza Comportamentale
Approccio Partecipativo
LA PAURA PIU GRANDE

Sicurezza Comportamentale

Il **fattore umano** come elemento **cardine della prevenzione**.

Psicologia della sicurezza: analisi del processo decisionale per comprendere e prevenire i comportamenti errati

Network and Information Security

Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity

The present report is concerned with human aspects of cybersecurity including not only psychology and sociology, but also ethnography, anthropology, human biology, behavioural economics and any other subject that takes humans as its main focal point.

Published April 16, 2019
Language English

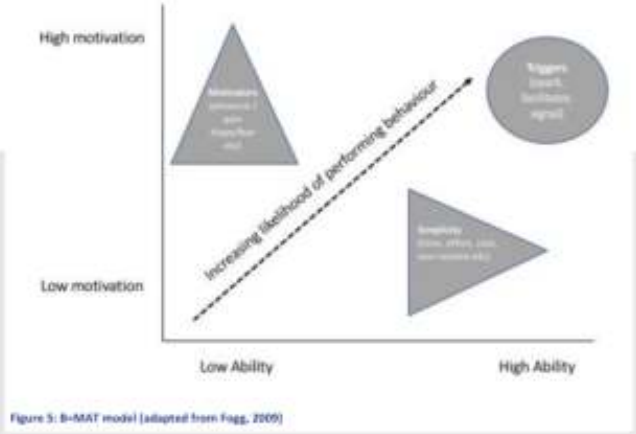


Figure 5: B=MAT model (adapted from Fogg, 2009)

Network and Information Security

Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity

The present report is concerned with human aspects of cybersecurity including not only psychology and sociology, but also ethnography, anthropology, human biology, behavioural economics and any other subject that takes humans as its main focal point.

Published April 16, 2019
Language English

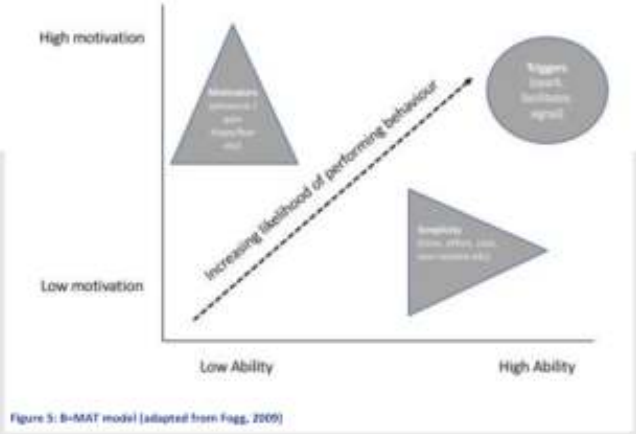


Figure 5: B=MAT model (adapted from Fogg, 2009)

Network and Information Security

Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity

The present report is concerned with human aspects of cybersecurity including not only psychology and sociology, but also ethnography, anthropology, human biology, behavioural economics and any other subject that takes humans as its main focal point.

Published April 16, 2019
Language English

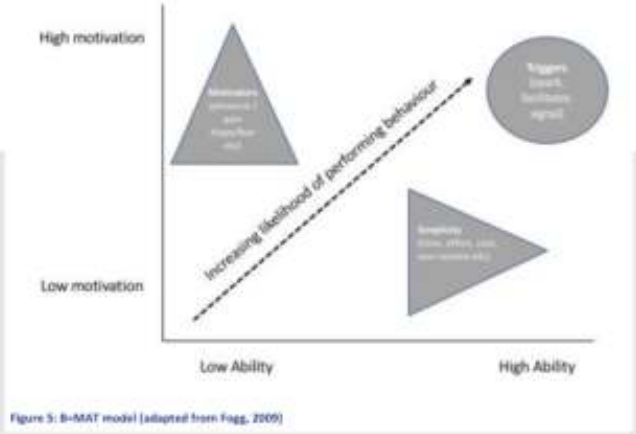


Figure 5: B=MAT model (adapted from Fogg, 2009)

Ergonomia

Ergonomia della sicurezza...
Ergonomia della protezione dei dati personali

Ergonomia cognitiva

Attenzione alle **differenze** e prevenzione basata sul modello umano di riferimento e su tutte le possibili eccezioni.

Cahier IP6 - La forme des choix

20 mars 2019

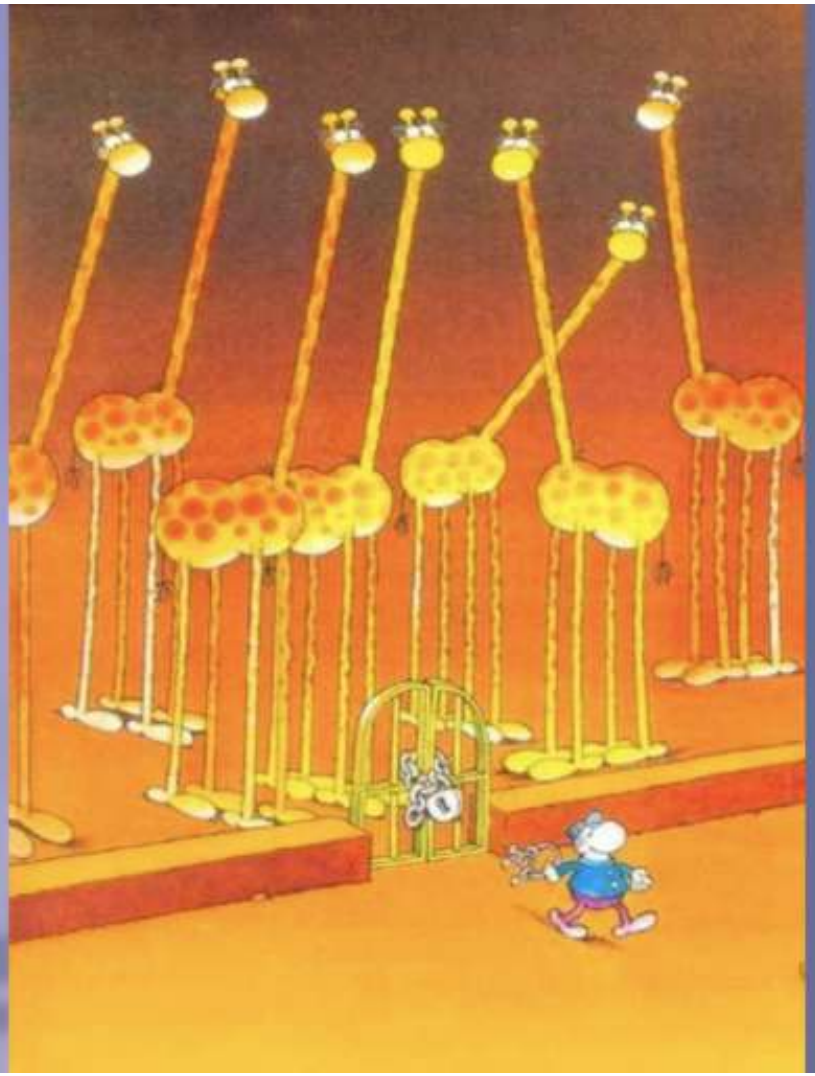
Le laboratoire d'innovation numérique de la CNIL (LINC) publie son 6ème cahier Innovation et prospective, *La Forme des choix - Données personnelles, design et frictions désirables* : une exploration des enjeux du design dans la conception des services numériques, au prisme de la protection des données et des libertés.

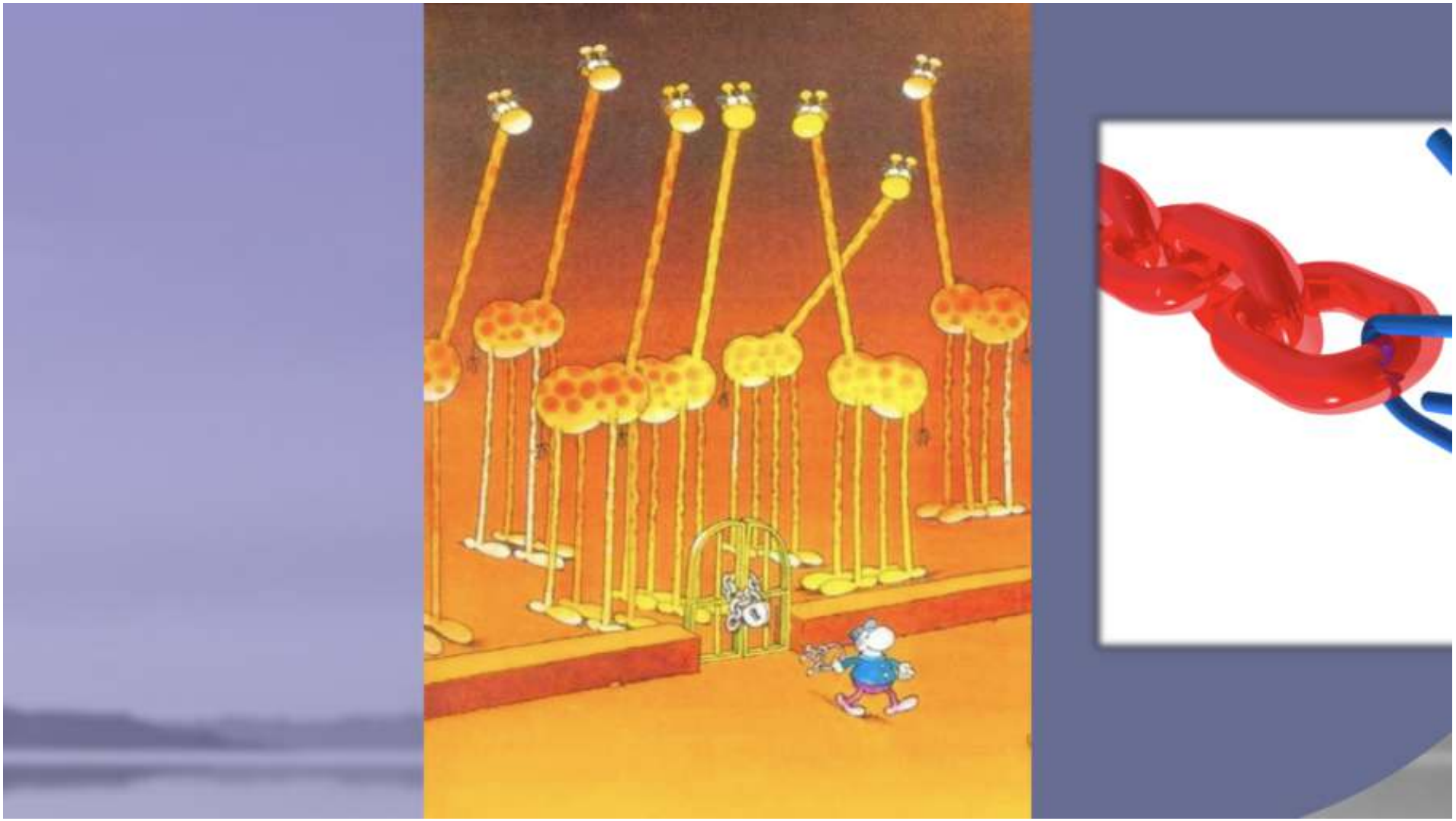
Le design des interfaces n'a pas attendu le Règlement général sur la protection des données (RGPD) pour influencer nos vies. Nous sommes depuis longtemps guidés dans nos déplacements et actions par des architectures de choix conçues et mise en œuvre par d'autres. La grande distribution a depuis longtemps modélisé son hypermarché avec des chemins préétablis visant à maximiser l'acte d'achat, depuis l'emplacement des packs d'eau à l'extrémité du magasin aux friandises disposées sur la caisse. Pourtant ces questions prennent un tour inédit dès lors qu'elles s'appliquent à des services numériques qui usent de méthodes de design pour parvenir à capter notre attention et traiter toujours plus nos données.

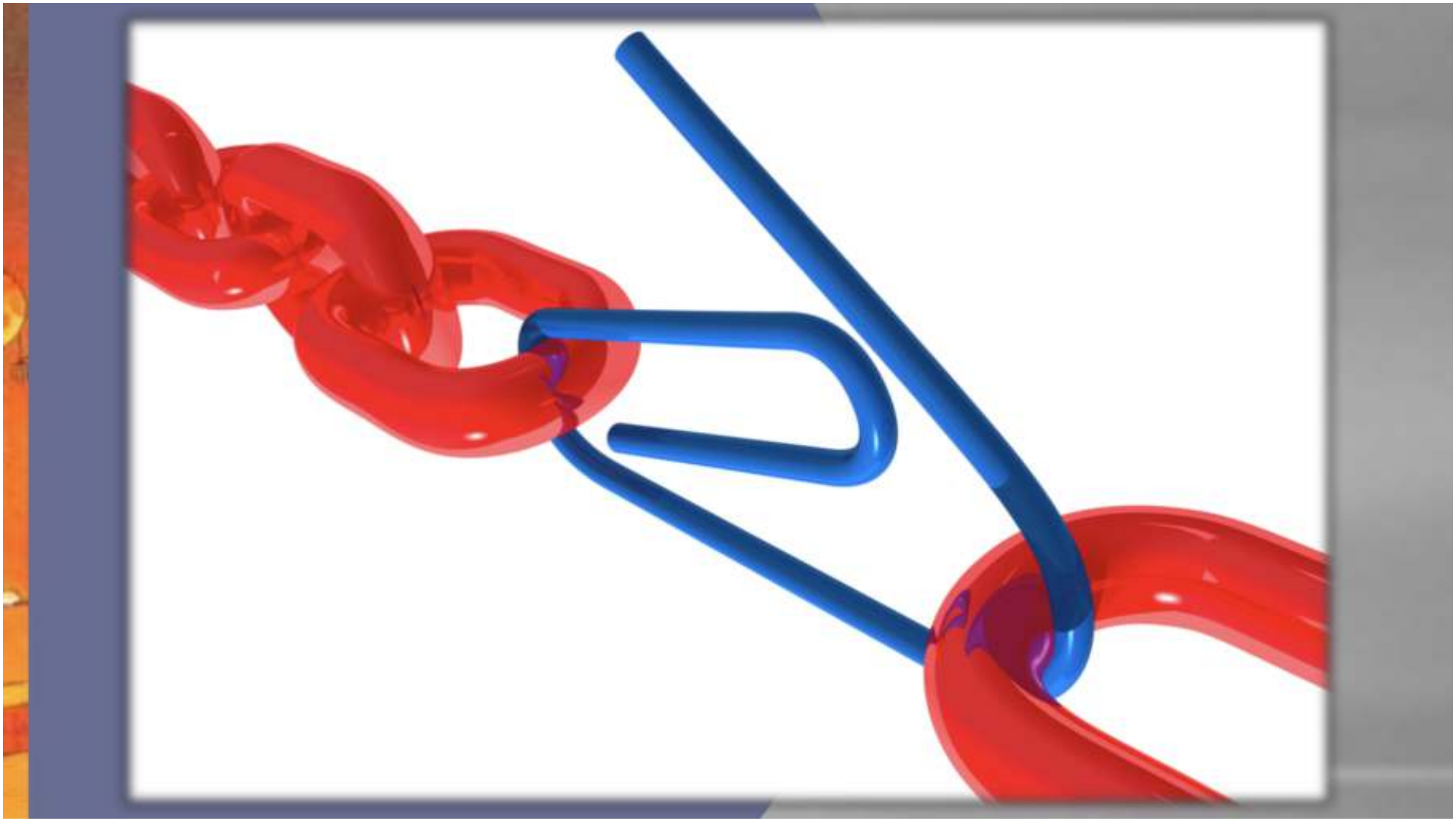

Mondo delle persone reali
"Standard" (uomo medio)
ABC


Data Protection Partecipativa

Data Protection Partecipativa





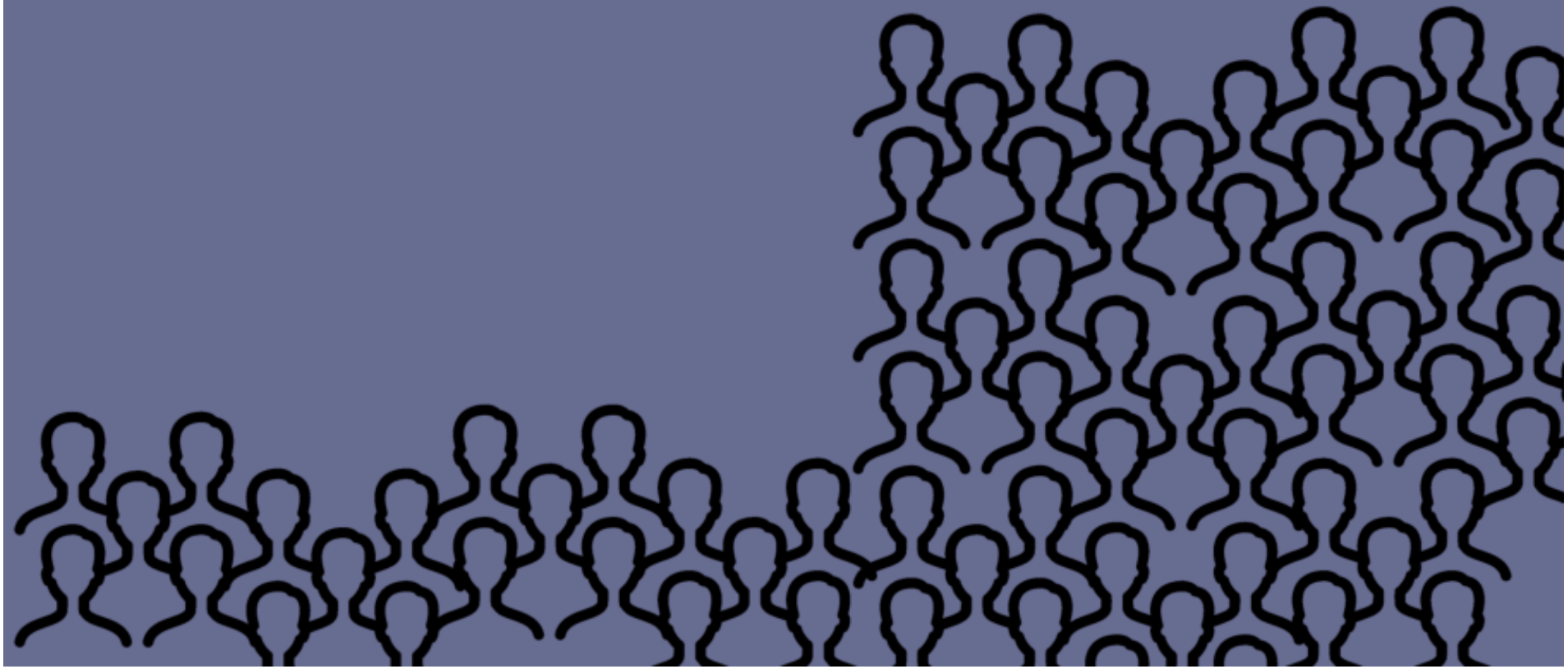


La paura più grande?

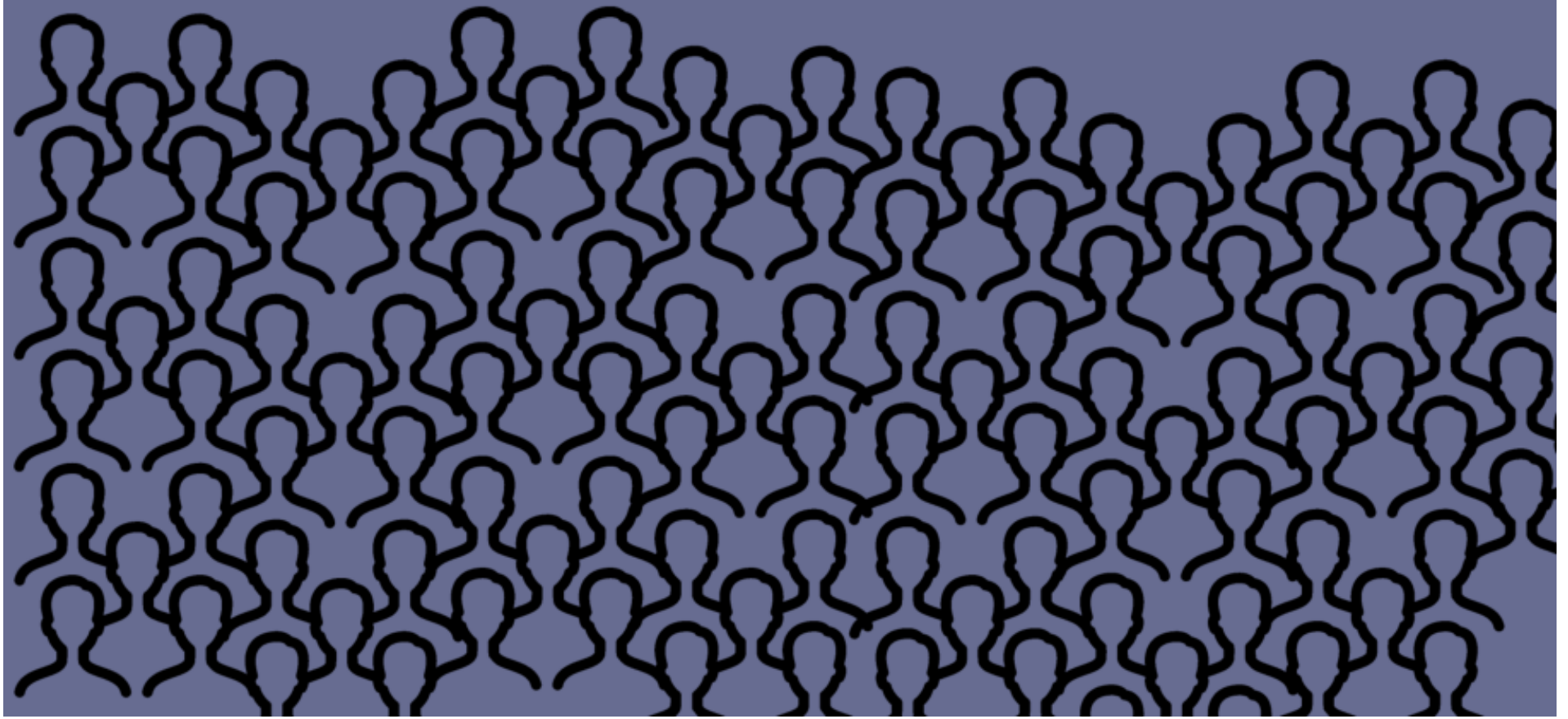




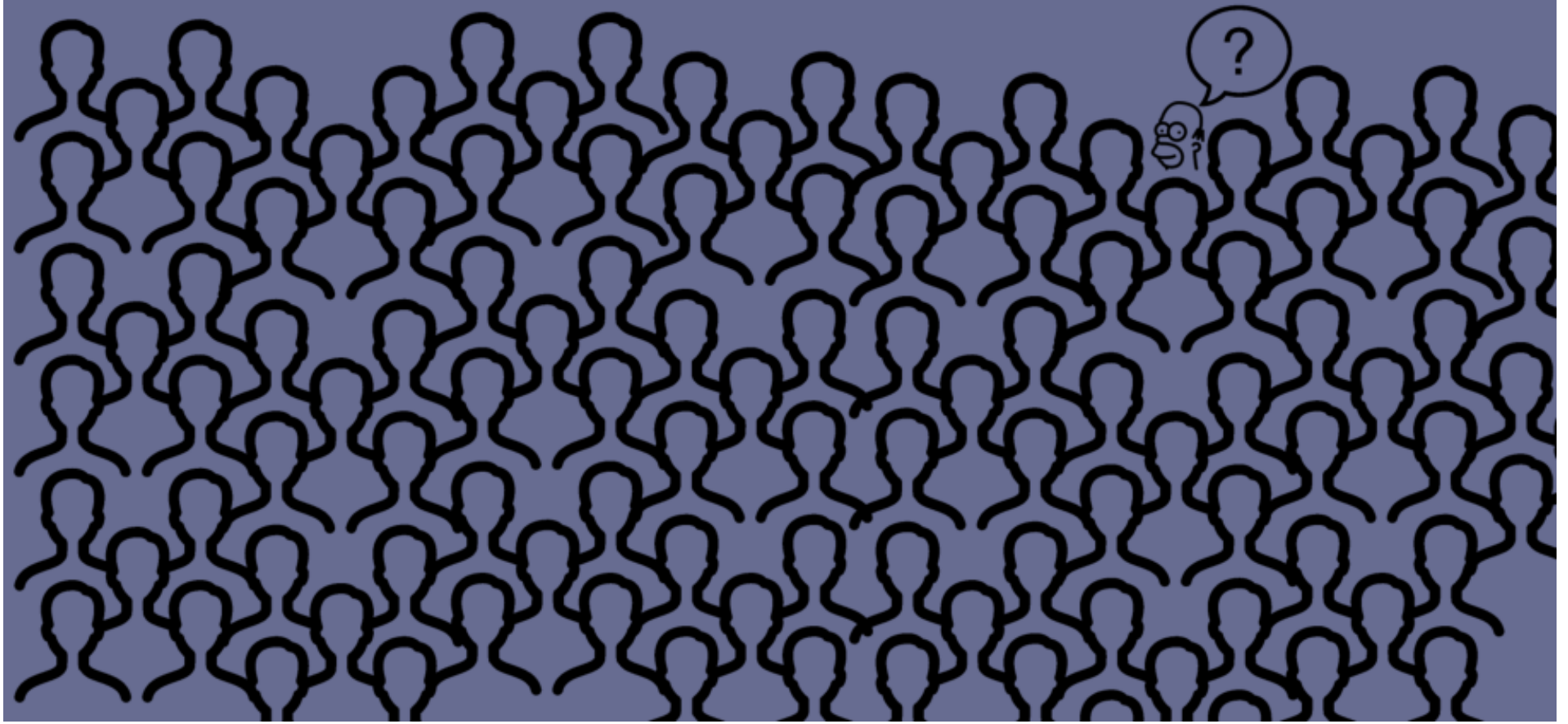

La paura più grande - 1

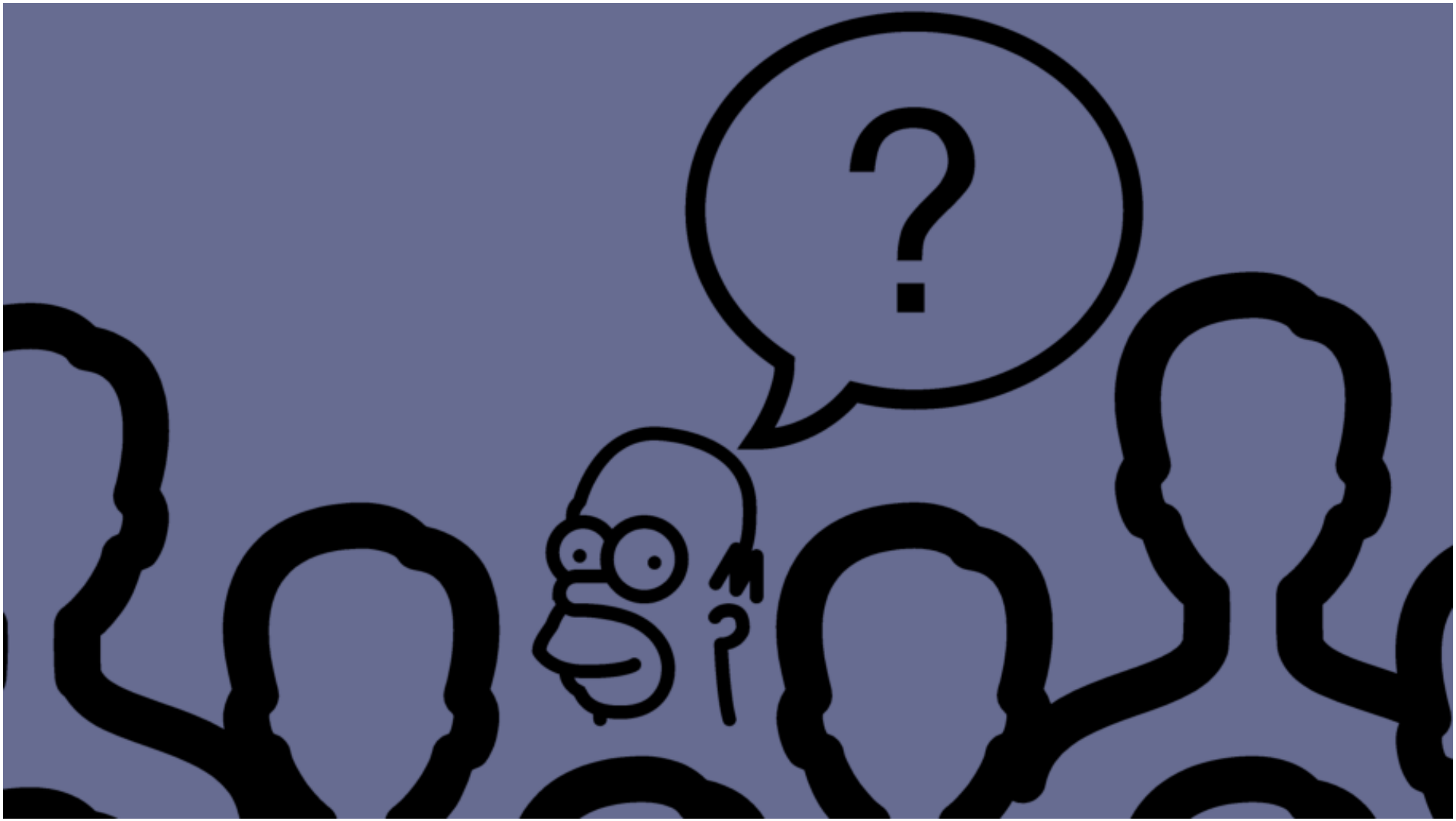


La paura più grande - 1



La paura più grande - 1

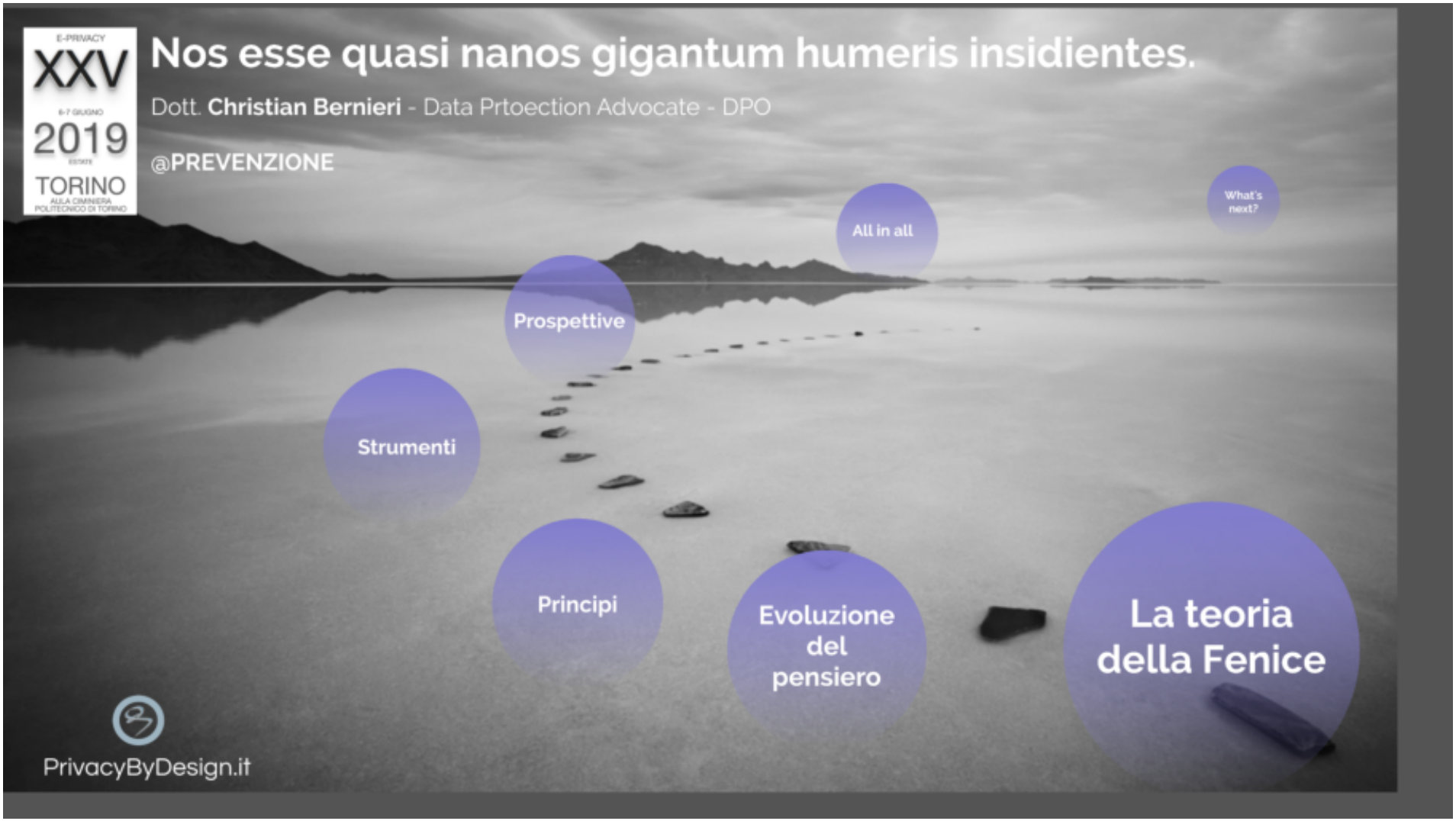




La paura più grande - 2

La paura più grande - 2

Dover rimediare!


E-PRIVACY
XXV
6-7 GIUGNO
2019
EDIZIONE
TORINO
AULA CIMINIERA
POLITECNICO DI TORINO
Nos esse quasi nanos gigantum humeris insidientes.
Dott. Christian Bernieri - Data Prtoection Advocate - DPO
@PREVENZIONE
What's next?
All in all
Prospettive
Strumenti
Principi
Evoluzione del pensiero
La teoria della Fenice
PrivacyByDesign.it