Mauro Mazzolari
Senior Consultant AGM
GRCteam

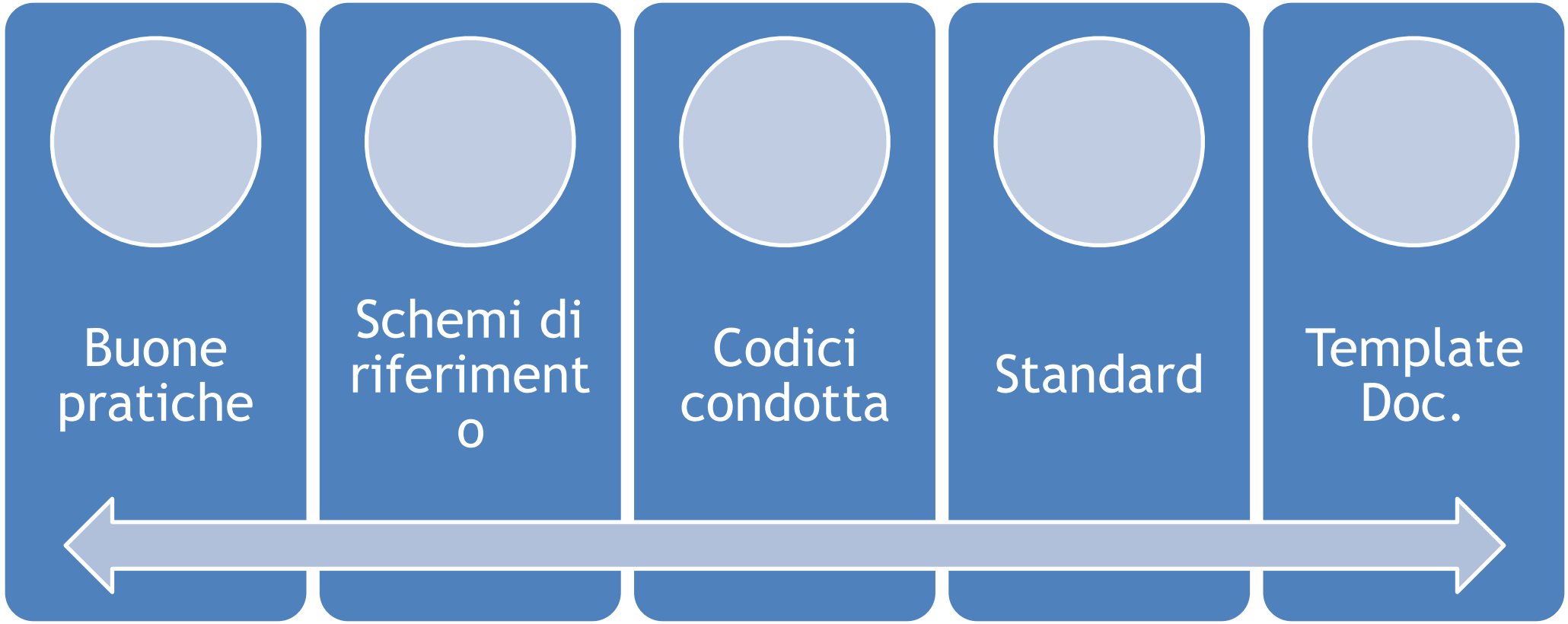
GDPR in pratica

Gestire la conformità Privacy in modo semplice

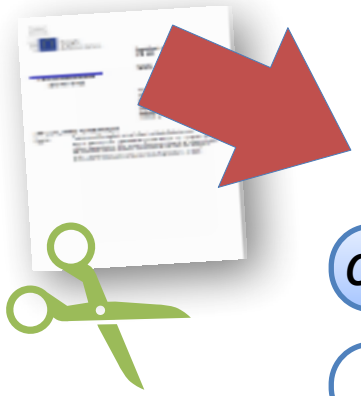
AREE DI INTERVENTO

OBIETTIVI FUNZIONALI

COSA ABBIAMO A DISPOSIZIONE



SCHEMA - GDPR



Interventi

Obb. Funzionale	Informazioni	Principi e policy	Processi e procedure	Ruoli e organizzazioni	Strumenti e servizi	Persone	Cultura, etica e comportamenti
Identificare	6.2, 8.1, 9, 28.3, 29, 32.4, 35, 36, 37, 49, 30 (I) , 6 , 30 , 30 , 9 , 30 (I) , 30 (I) , 30 (I) , 24, 26, 27, 28, 30 , 30 , da 44 a 49 , 30 , 32, 35 , 32 , 35 , 33--34	5		37, 24, 28, 29, 29, 26, 27	32 (I)	29, 32, 39	**, *, *
Proteggere	13-14, da 6 a 10; 22, 26_27_28, 30, da 45 a 48, 45, 47, 46 c.2 lett. d), 46, 46 c.3 lett. a), 49, 12, da 15 a 21, 57	5, 5, 24, 12, 32, 5 c.1 lett.d), 32 c.2 , 6 c.4 , 8, 9, 10, 28, 12 (I),	5, 32, 35, 12; da 15 a 21, 33 - 34, 33-34, 32, 24; 32; 35, 5 c.1 lett.d), 15, 8, 25, 35, 24, 32, 32, 32 (S), 32 (S), 32 (S), 32 (S), 32, 44, 47, 46 , 46, 46 , 49	26-27-28-37	32, 32 (I), 33 (I),	29, 39, 42,	
Monitorare e Rilevare	24, . da 15 a 21 (S), . 33 (S); 34 (S), . 35(S), . 25 (S),		24, 32, 32, 24, 12, 57, 12; da 15 a 21, 57 (I)	28	5, 24, 32 (I); 33 (I),		
Rispondere			24, 25, 33, 34, 25, 12, 15, 21, 17, 18, 21, 21, 21, 21, 20, 16, 7, 24, 35, 32; 35, 32; 35, 13 - 14, 6-7-8-9-10-22, 26-27-28-37, 42,				
Recuperare			24 - 25, 32, 32, 5				

- *Obbligatorio*
- *Implicito*
- *Supporto*

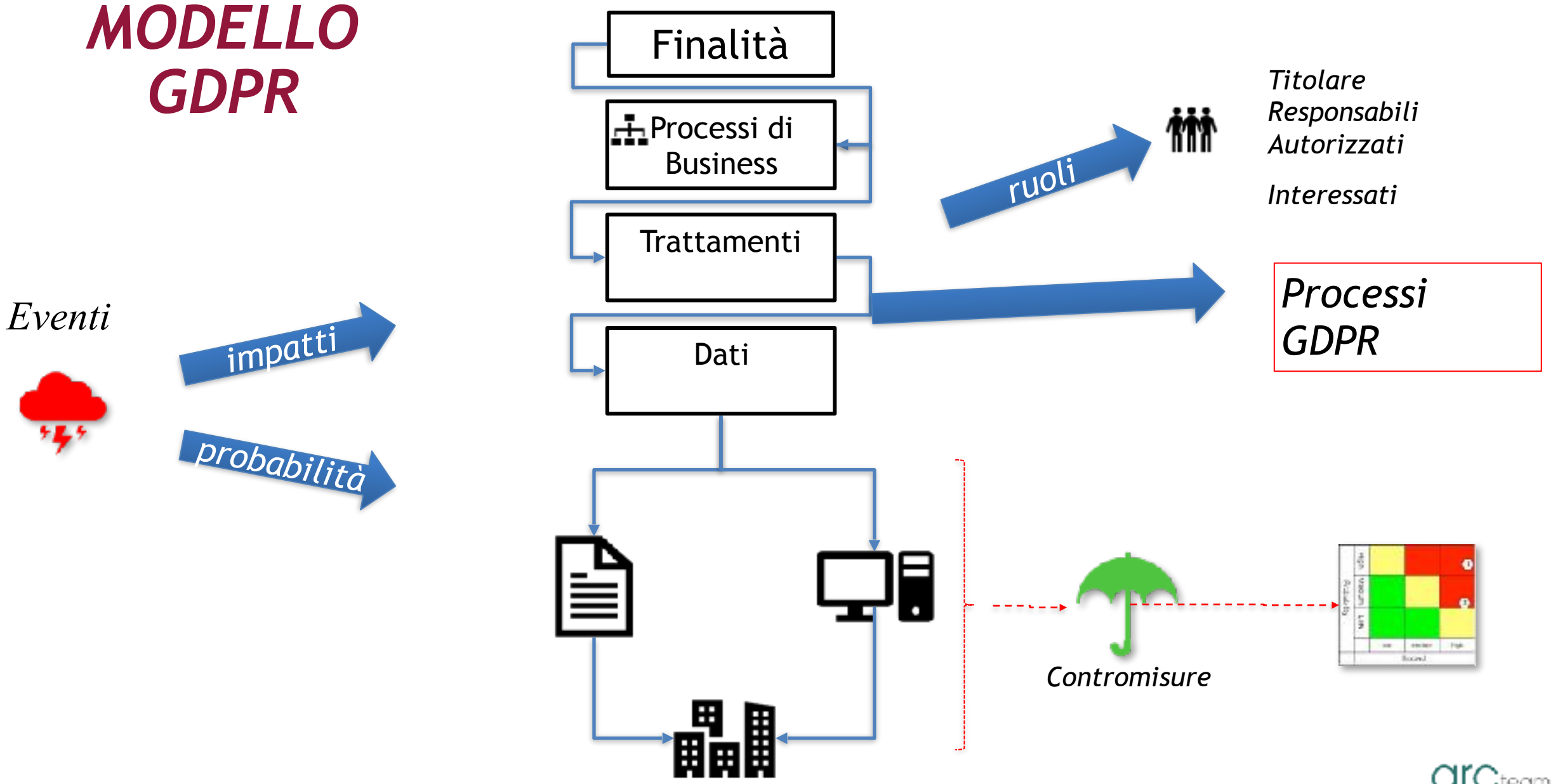
Come

- Buone pratiche
- Standard
- Framework
- Sigilli
- Codici condotta
- Certificazioni
- Capability Maturity
- Template Doc.
-

KEYMAP

grc team

MODELLO GDPR



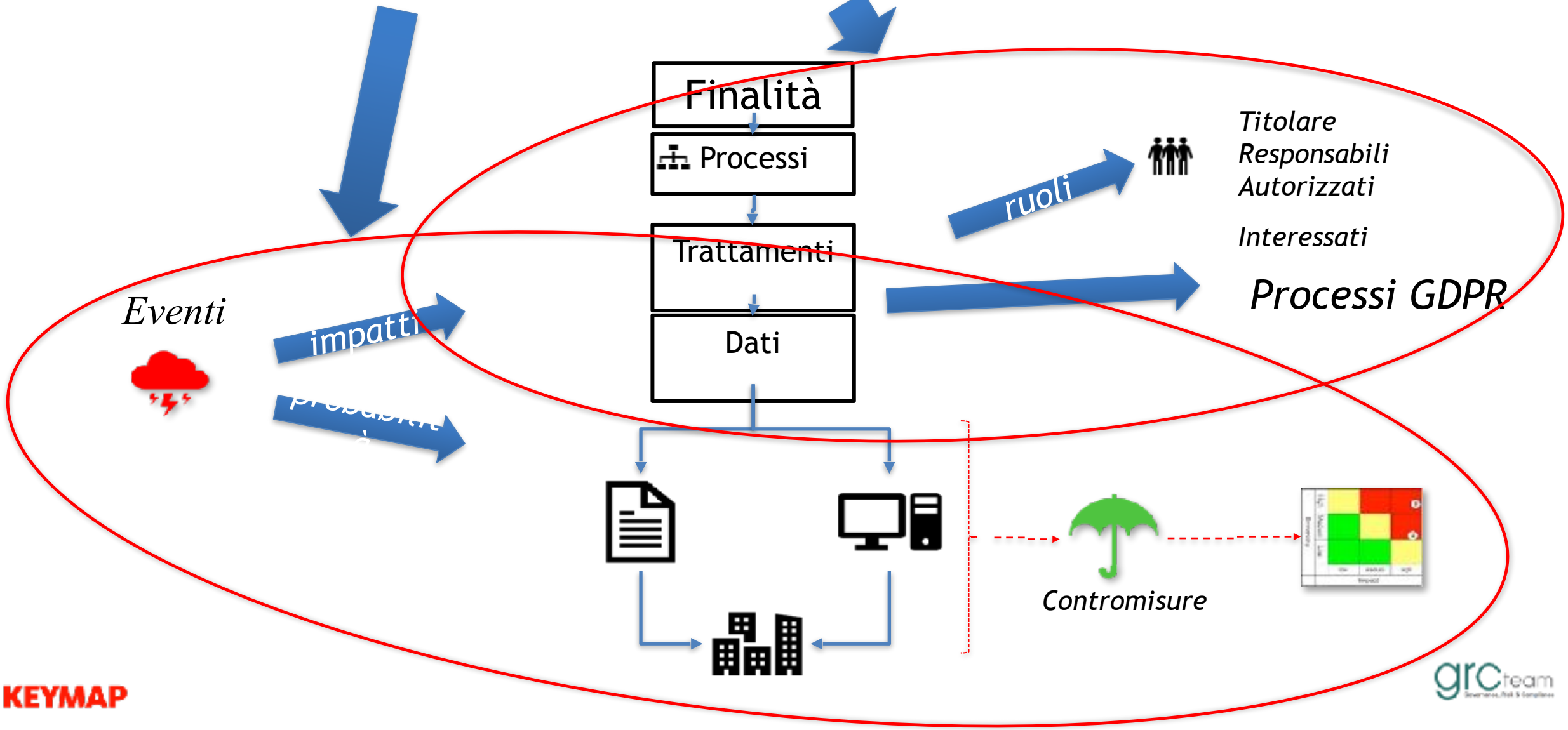
KEYMAP

grc team

Gestione dei rischi sui «Dati Personali»

Tutela dei diritti e delle libertà delle persone fisiche

CONFORMITÀ AL GDPR

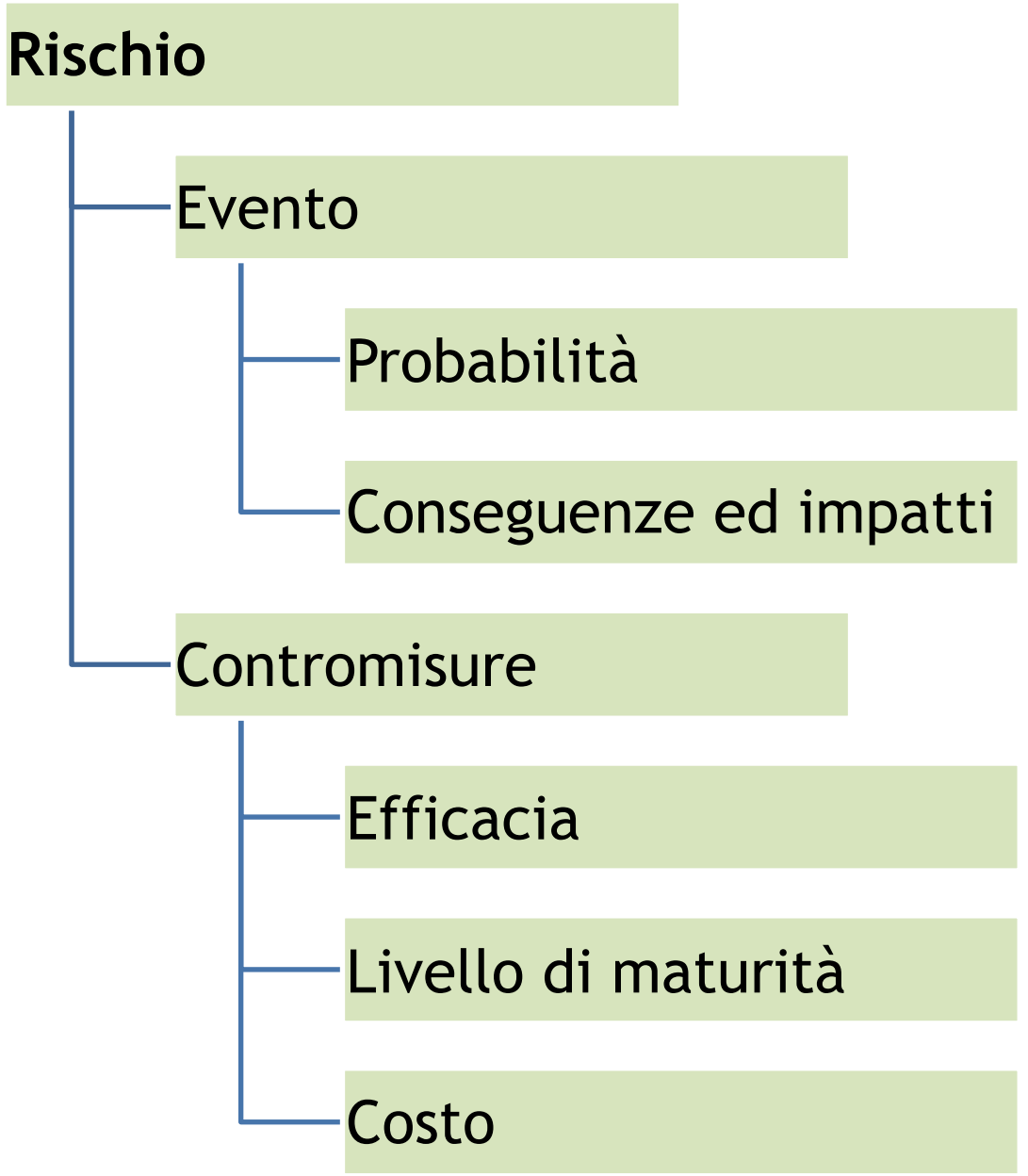


KEYMAP

grc team

Sicurezza e rischio

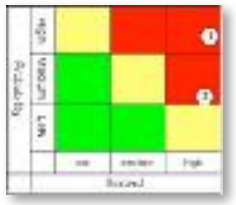
- Sicurezza è :
- consapevolezza e comprensione dei rischi
- Capacità di gestirli

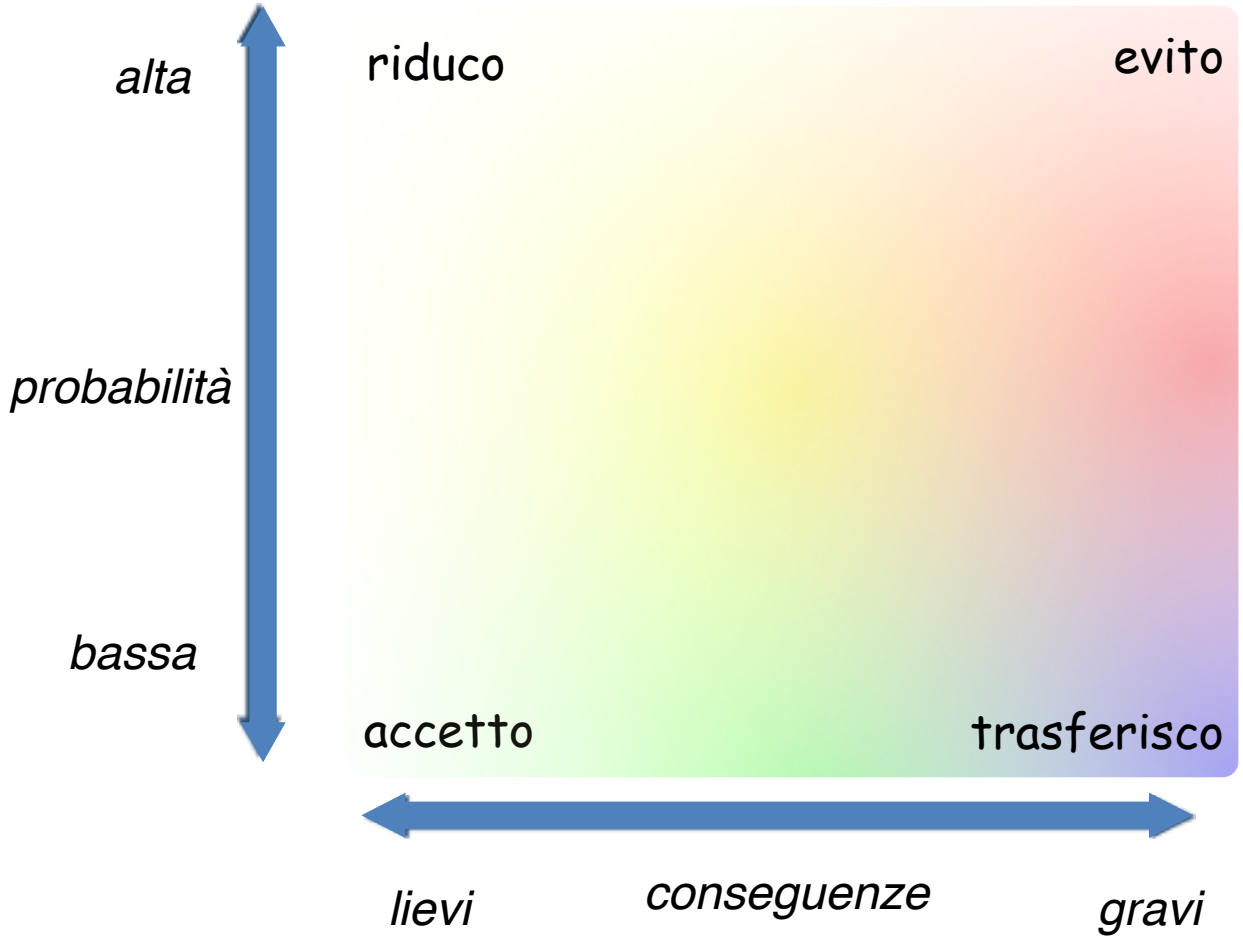


KEYMAP

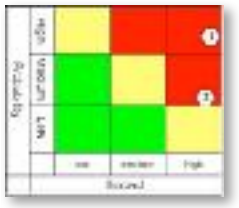
grc team

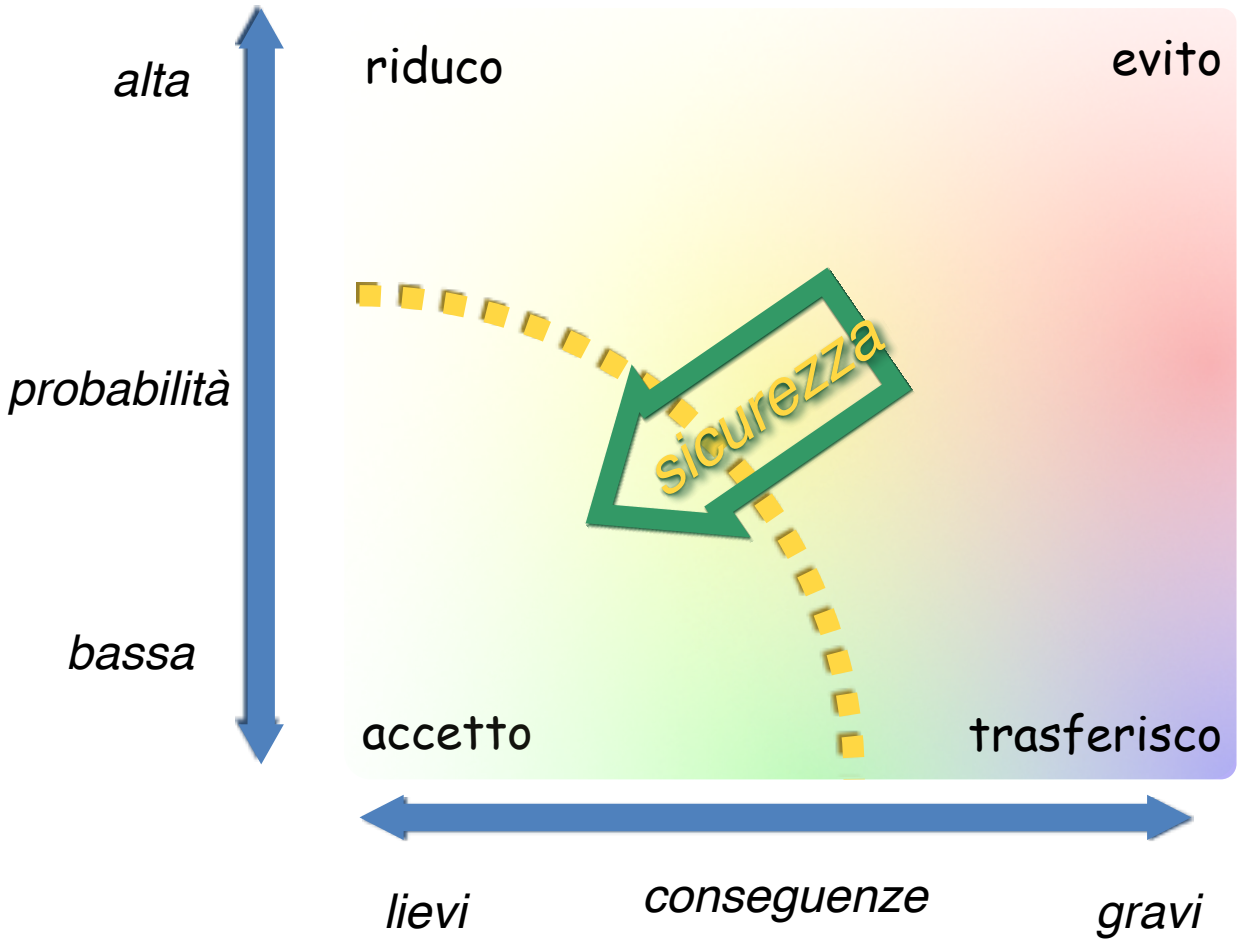
Gestione del Rischio





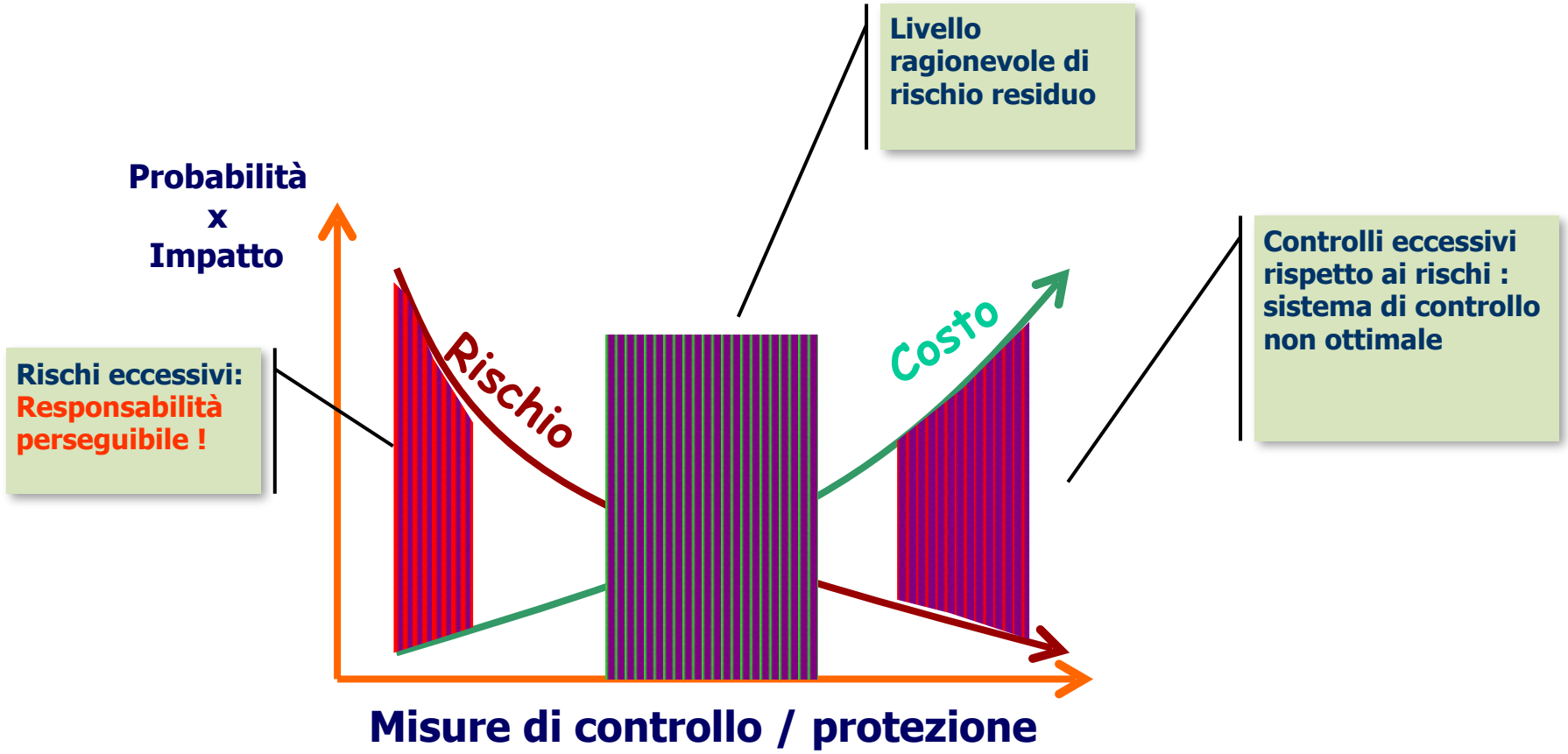
Gestione del Rischio





- Equilibrio tra costi e benefici

Misure adeguate



Gestione del rischio

Elusione rinuncia all'attività

Prevenzione riduzione della probabilità dell'evento

Protezione minimizzare le conseguenze ad evento avvenuto

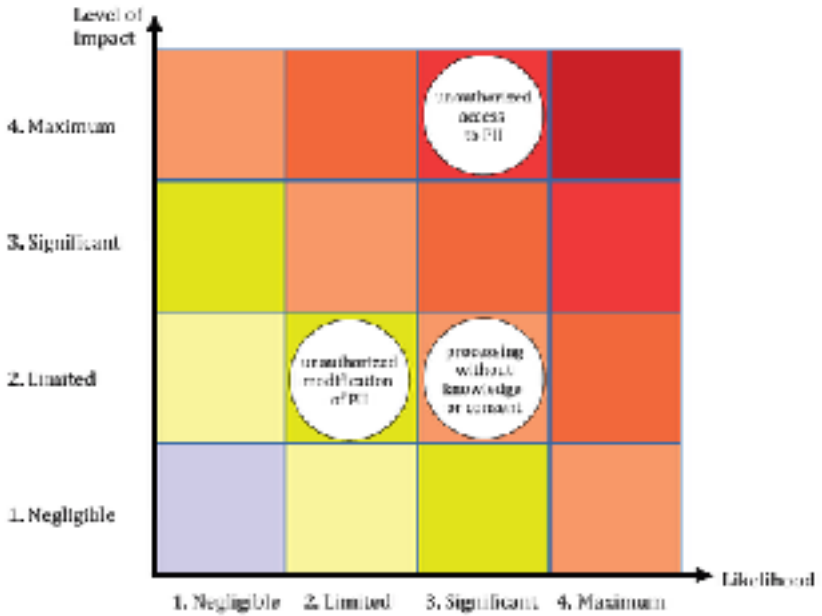
Trasferimento

- **Assicurativo**
- **Non assicurativo (contrattuale, LdS)**

Ritenzione

- Consapevole
- Inconsapevole
  - Mancata identificazione del rischio
  - Sottovalutazione dell'entità del rischio
  - Sopravvalutazione dell'efficacia delle misure

ISO/IEC 2910(
ISO/IEC 2913
ISO/IEC 2915



Impatto	
Molto alto	Gli interessati possono incontrare proplemi significativi, o anche conseguenze irreversibili e non superabili (incapacità di lavorare a lungo termine, psicologico o disturbi fisici, morte, ecc.).
Alto	Gli interessati possono incontrare notevoli conseguenze superabili solo anche se con gravi difficoltà (appropriazione indebita di fondi, blacklist da istituzioni finanziarie, i danni alla proprietà, la perdita di occupazione, citazione in giudizio, il peggioramento della salute, ecc.).
Medio	Gli interessati possono incontrare inconvenienti superabili con qualche difficoltà (costi extra, impossibilità temporanea di accesso ai servizi di business, di preoccupazioni e timori ed incomprensioni, stress, minori fastidi fisici, ecc.).
Basso	Gli interessati possono incontrare piccoli inconvenienti superabili senza particolari problemi (perdita di tempo per re-inserimento di dati, fastidi, irritazioni, ecc.).

Probabilità	
Massima	ad esempio il furto di documenti cartacei archiviati in una sala d'attesa
Significativa	ad esempio il furto di documenti cartacei archiviati negli uffici cui si accede senza controllo
Limitata	ad esempio il furto di documenti cartacei archiviati in un ambiente con accesso controllato con di badge
Trascurabile	ad esempio il furto di documenti cartacei archiviati in un ambiente protetto da un lettore di badge e il codice di accesso

Misura delle probabilità

ENISA

europa.eu

Guidelines for SMEs on the security of personal data processing

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
NETWORK AND TECHNICAL RESOURCES	☐ Low	1
	☐ Medium	2
	☐ High	3
PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA	☐ Low	1
	☐ Medium	2
	☐ High	3
PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA	☐ Low	1
	☐ Medium	2
	☐ High	3
BUSINESS SECTOR AND SCALE OF PROCESSING	☐ Low	1
	☐ Medium	2
	☐ High	3

KEYMAP

grc team

Esposizione a minacce (per il contesto considerato)

ENISA europa.eu

A. Rete e le risorse tecniche		Si/ No
1	Una parte qualsiasi dei trattamenti di dati personali è effettuata tramite internet?	
2	Il personale interno può accedere al sistema di elaborazione di dati tramite la connessione internet (ad esempio per alcuni utenti o gruppi di utenti)?	
3	Il trattamento dei dati personali avviene tramite un sistema interconnesso ad un sistema o servizio esterno o interno (per la vostra organizzazione)?	
4	Un utente non autorizzato può accedere facilmente al sistema di elaborazione dati?	
5	Il sistema di trattamento dei dati personali è stato progettato, implementato o mantenuto senza le best practice documentate indicate al punto seguente?	

B. Processi e procedure relative al trattamento dei Dati Personali		Si/ No
6	I ruoli e le responsabilità relative al trattamento dei dati personali sono vaghi o non sono chiaramente definiti?	
7	L'uso accettabile di rete, sistemi e risorse fisiche all'interno dell'organizzazione è ambiguo o non è chiaramente definito?	
8	I dipendenti sono autorizzati a portare e usare i propri dispositivi per collegarsi ai sistemi che trattano i dati personali?	
9	I dipendenti sono autorizzati a trasferire, memorizzare o altrimenti trattare i dati personali al di fuori dei locali dell'organizzazione?	
10	I dati personali possono venir trattati senza la creazione di file di log?	

C. Parti/persone coinvolte nel trattamento dei Dati Personali		Si/ No
11	Il trattamento dei dati personali effettuato da un numero indefinito di dipendenti?	
12	È una parte qualsiasi del trattamento dei dati è eseguita da un contraente / terzi (responsabile del trattamento)?	
13	Gli obblighi delle parti/persone coinvolte nel trattamento dei dati personali sono definite in modo ambiguo o non chiaramente ?	
14	Il personale coinvolto nel trattamento dei dati personali non ha dimestichezza con le questioni relative alla sicurezza ?	
15	Il personale coinvolto nel trattamento non adotta opportune misure di conservazione e/o distruzione sicura dei dati personali?	

D. Settore di attività e la scala di elaborazione		Si/ No
16	Ritieni il tuo settore di attività esposto ad attacchi alla sicurezza informatica?	
17	Il settore in esame ha subito un qualsiasi attacco informatico o altro tipo di violazione della sicurezza nel corso degli ultimi due anni?	
18	Avete ricevuto alcuna notifica e/o reclami per quanto riguarda la sicurezza del sistema IT (utilizzata per il trattamento dei dati personali) nel corso dell'ultimo anno?	
19	Le operazioni di trattamento riguardano riguardano grandi volumi di interessati e/o di dati personali?	
20	Nel il vostro settore di attività esistono delle best practice di sicurezza che non vengono adeguatamente rispettate?	

Contesto dei trattamenti

ENISA

AREA DI VALUTAZIONE	Probabilità	
	Livello	Valore
La rete e le risorse tecniche	Bassa	1
	Medie	2
	Alta	3
Processi e procedure RELATIVE AL TRATTAMENTO DEI DATI PERSONALI	Bassa	1
	Medie	2
	Alta	3
Parti/PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	Bassa	1
	Medie	2
	Alta	3
Settore di attività e la scala di elaborazione	Bassa	1
	Medie	2
	Alta	3

Valore totale	Probabilità che un evento dannoso si verifichi
4 - 5	Bassa
6 - 8	Media
9 -12	Alta

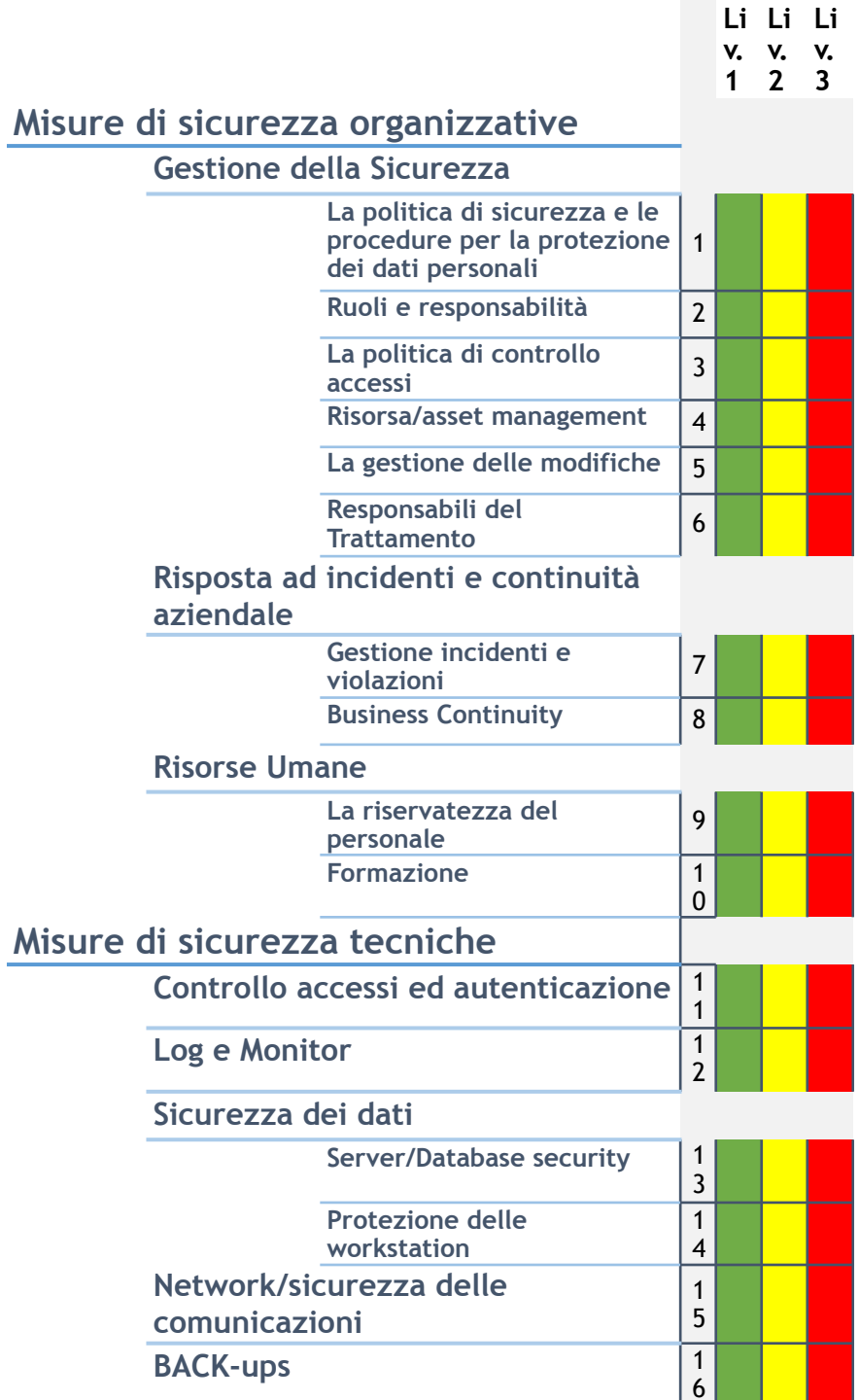
KEYMAP

grc team

Contesto: il Profilo di rischio «specifico»

		Livello di impatto sull'interessato		
		Basso	Medio	Alto / Molto alto
Probabilità di occorrenza di un evento	Bassa			
	Media			
	Alta			

Livello complessivo di «maturity» delle misure da adottare (o già in essere !)



ENISA

europa.eu

Rif. a standard (ISO 27001)

KEYMAP

grc team

Obiettivo : Elaborare un Framework per il GDPR

- Creare un modello che per costruire un «Progetto Privacy»
  - Un unico schema integrato
  - Definire e dimostrare , per il contesto in esame, la conformità al GDPR (o i piani di adeguamento)
- Confronto con quanto viene fatto nelle altre nazioni EU
- Applicare linee guida ENISA (1)
- Attenzione a linee guida e suggerimenti del WP29 (EDPB)
- *Finally, the WP29 appointed among its members a representative for the next ENISA Permanent Stakeholders Group(12 10 2017)*

1- AGENZIA DELL'UNIONE EUROPEA PER LA SICUREZZA DELLE RETI E DELL'INFOR ONE

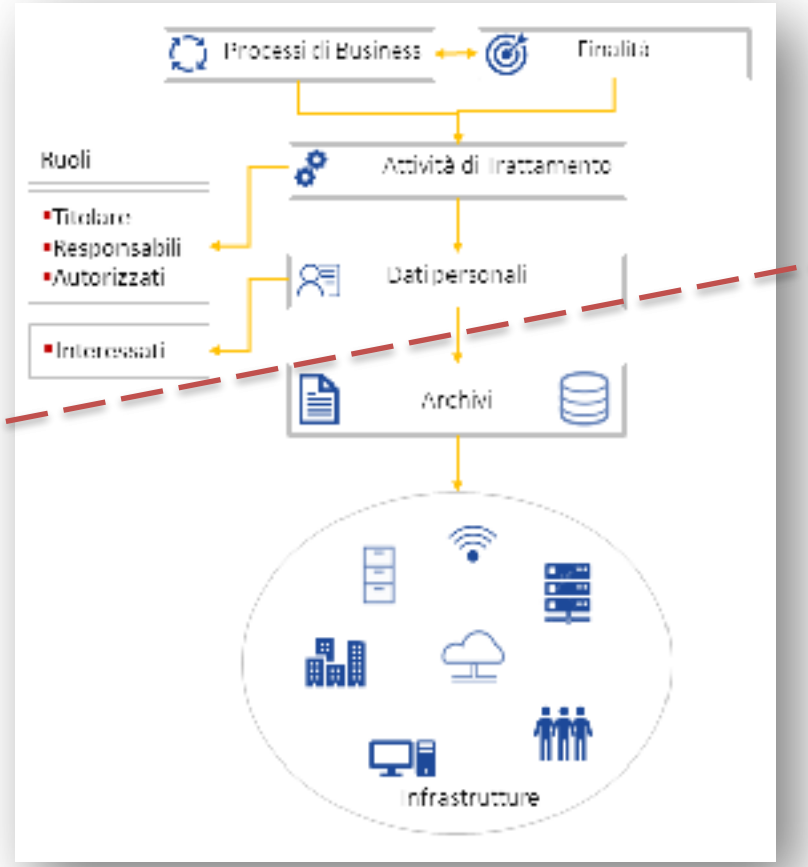
Il WP29 incoraggia lo sviluppo di quadri di valutazione d'impatto sulla protezione dei dati specifici dei vari settori.

Ciò è dovuto al fatto che essi possono attingere a conoscenze specifiche settoriali, aspetto questo che fa sì che la valutazione d'impatto sulla protezione dei dati possa affrontare le specificità di un particolare tipo di trattamento (ad esempio tipi particolari di dati, risorse aziendali, impatti potenziali, minacce, misure).

Ciò significa che la valutazione d'impatto sulla protezione dei dati può affrontare le problematiche che sorgono in un settore economico specifico oppure quando si utilizzano tecnologie particolari o si eseguono tipologie particolari di trattamento.

Simile per settore

Specifico per Azienda



RACCOLTA DATI

Processi		
1	2	3
Processi 1	Processi 2	Processi 3

RACCOLTA DATI

Attività di Trattamento						
			Ruoli			
4	5	6	7	8	9	10
Att. Trattamento	Descrizione	Finalità Tratt.	Titolare	Responsabili interni	Responsabili esterni	Autorizzati

RACCOLTA DATI

(PII)Dato personale								
						Impatto		
11	12	122	13	14	142	15	16	17
Nome PII	Tipo dato pers.	Descrizione2	Interessati	Categoria interessati	Raccolta presso int.	R	I	D

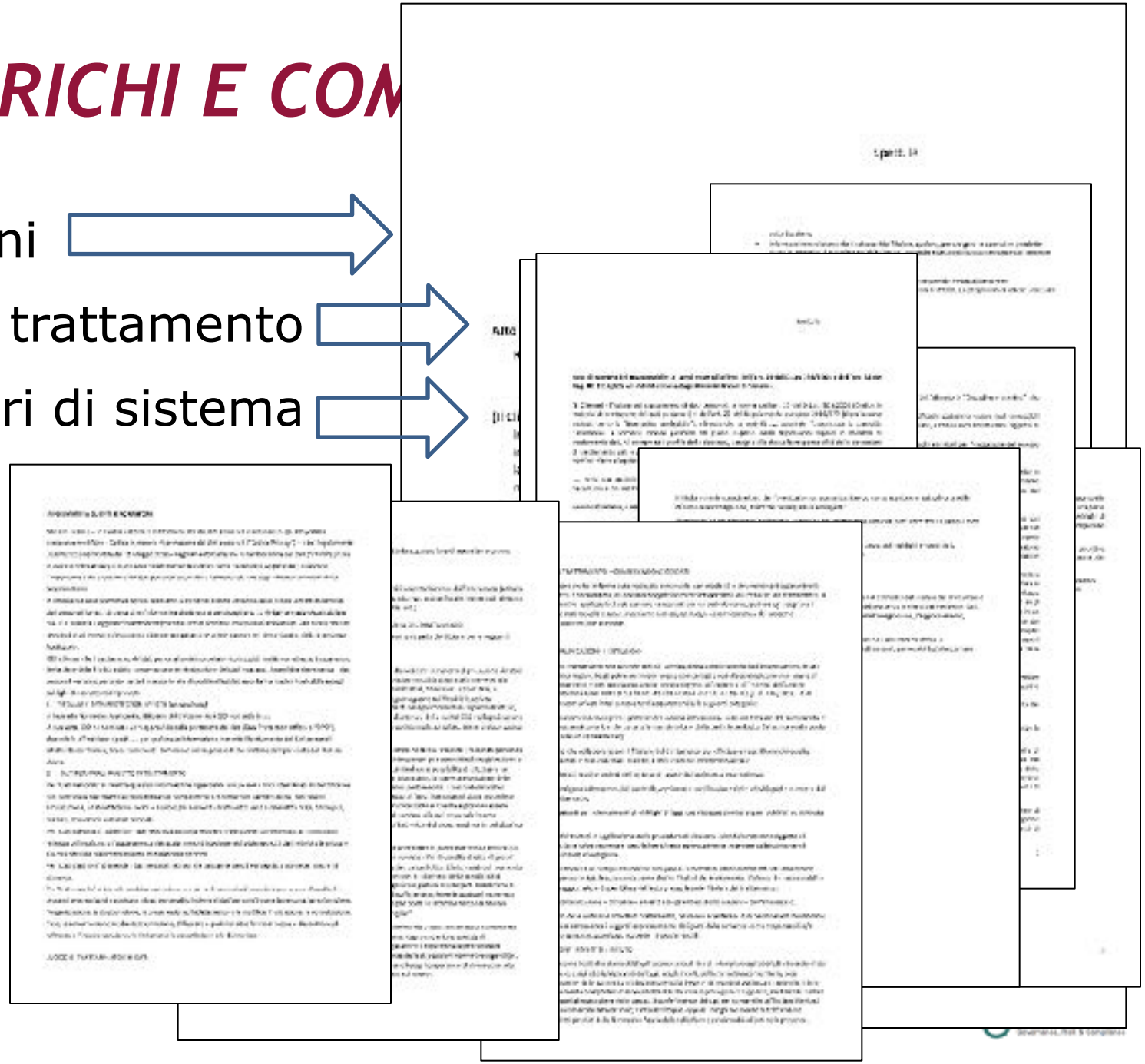
(PII)Dato personale						
Data Breach		Conservazione				
18	19	20	202	21	22	222
T	EI	Tempo	Criteri	Destinatari	Trasf. No UE	Modalità trasferimento

RACCOLTA DATI

Archivio informatizzato					Archivio non automatizzato	
		Piattaforme IT di riferimento				
23	24	25	26	27	28	29
Archivio IT	Applicazioni di riferimento	Server /PC	Sistema operativo	DB	Archivio no IT	Supporto

RUOLI, INCARICHI E COM

- Nomina Responsabili esterni
- Incarichi agli autorizzati al trattamento
- Incarichi agli amministratori di sistema
- Raccolta del consenso
- Informativa



Risorse		Contesto		Livello di sicurezza richiesto	Area	Controlli		
		Nome	Liv. criticità			adottati -->	<-- da adottare	Progetto di adeguamento
Rete		Contesto Ax	Medio	Basso	Network/sicurezza di comunicazione	C.1 C.3 C.4		
Archivi fisici	Armadio ingresso	Contesto Ax	Medio	Medio	Sicurezza fisica	T.1 T.2 T.4 T.6 T.7 T.8	I.3 I.5	
	Arm. Amministrazione	Contesto Ax	Medio	Medio	Sicurezza fisica	I.1 I.2 I.4 I.6 I.7 I.8	I.3 I.5	
	Arm. Amministrazione	Contesto Ax	Medio	Medio	Sicurezza fisica	T.1 T.2 T.4 T.6 T.7 I.8	I.3 I.5	
	Arm. Personale	Contesto Ax	Medio	Medio	Sicurezza fisica	I.1 I.2 I.4 I.6 I.7 I.8	T.3 T.5	
	Arm. Personale (Il saldone personale)	Contesto Ax	Medio	Medio	Sicurezza fisica	I.1 I.2 I.4 I.6 I.7 T.8	I.3 I.5	
Cloud		n.d.	n.d.	n.d.	Network/sicurezza di comunicazione			
Sistemi operativi / DB		n.d.	n.d.	n.d.	Server/Database security			
Azienda / struttura organizzativa		Contesto Ax	Medio	Basso	La politica di sicurezza e le procedure per la protezione dei dati personali	A.1 A.2 A.3 A.4		
					Ruoli e responsabilità	B.1 B.2 B.3 B.4 B.5		
					La politica di controllo di accesso	C.1 C.2		
					Risorse/asset management	D.1 D.2 D.3 D.4		
					La gestione delle modifiche	L.1 L.2		
					Responsabili del trattamento	H.1 H.2 H.3 H.4		
					Gestione incidenti e violazioni	G.1 G.2 G.3 G.4		
					Business Continuity	H.1		
					Logs e Monitor	L.1 L.2 L.3 L.4 L.5		
Dispositivi mobili/portatili		Contesto Ax	Medio	Basso	Dispositivi mobili / portatili	Q.1 Q.2 Q.3 Q.4 Q.7 Q.8		

I «Processi» GDPR

Acquisizione consenso o equivalente		
Data Protection Management self assessment		
Data Protection Risk Assessment		
Designazione ruoli		
DPIA		
Rilascio informative		
Data Breach Notification		
Rispetto Diritti dell'Interessato : rispondere e registrare		
	Accesso	
	Modifica/rettifica	
	Diritto all'oblio	
	Limitazione del trattamento	
	Portabilità dati	
	Opposizione	
	Utilizzo per decisioni automatizzate	
Rilevare ,monitorare e registrare		
	Eventi «Privacy»	
	Eventi che comportano modifiche al sistema protezione dati e rilascio di nuove informative, designazioni… con conseguente aggiornamento del Modello GDPR	

come realizzarli e come dimostrarne la «Capability» per ogni «trattamento / dato» ?

KEYMAP

grc team

Tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati

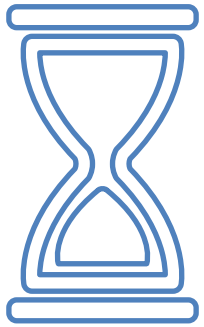
Rispetto diritti interessato

Nome	Cat.	DB/doc.	Livello di Sicurezza	Trattamento	Diritti dell'interessato								
					Art. 7 - Acquisizione consenso o equivalente, e revoca	Art.13 e 14 Informativa	Art.15 - Accesso al dato	Art.16 - Modifica / rettifica	Art.17 - Diritto all'oblio	Art.18 - Limitazione del trattamento	Art.20 - Portabilità dei Dati	Art.21 Opposizione	Art.22 - Utilizzo per decisioni automatizzate
Anagrafiche ASTOR(Art00)	Norm.	1	Medio	Gestione anagrafiche	✓	✓	✓	✓	✓	✓	✓	✓	
Applicativo gestione arrassi Zucchelli(Art40)	Norm.	1	Medio	Gestione accessi dipendenti	✓	✓	✓	✓			✓	✓	✓
				Gestione accessi fornitori/consulenti	✓	✓	✓			✓	✓	✓	✓
Archivio contatti(Art5)	Norm.	1	Basso	Gestione contatti agenti/mechanicien	✓	✓	✓	✓	✓	✓	✓	✓	✓
				Gestione contatti clienti	✓			✓	✓	✓	✓		✓
				Gestione contatti fornitori	✓		✓	✓		✓	✓	✓	✓
				Gestione logistica e programmazione		✓							✓
Database concorsi consumatori (esterno)(Art10)	Norm.	1	Medio	Gestione concorsi consumatori	✓	✓							✓
Database contatti sito e-Boutique(Art01)	Norm.	1	Medio	Gestione sito e Boutique	✓	✓							✓
Database contatti sito Cyquyque(Art39)	Norm.	1	Basso	Gestione sito istituzionale Cyquyque	✓								✓
Database contatti sito spazio Cyquyque/ IrMa(Art16)	Norm.	1	Basso	Gestione sito istituzionale spazio Cyquyque/IrMa	✓	✓							✓
Database contatti sito TMR(Art23)	Norm.	1	Medio	Gestione sito istituzionale TMR	✓	✓	✓		✓	✓	✓		✓
Database registrati Newsletter Divisione Retail(Art17)	Norm.	1	Basso	Gestione Newsletter Divisione Retail	✓	✓	✓	✓	✓		✓	✓	
Database registrati Newsletter Cyquyque(Art19)	Norm.	1	Basso	Gestione Newsletter Cyquyque	✓	✓	✓		✓	✓	✓	✓	
Database utenti Active Directory(Art27)	Norm.	1	Medio	Gestione profili utenti e risorse		✓	✓		✓	✓	✓	✓	✓
Data archiviazione ottica(Art52)	Norm.	1		Nessun trattamento									

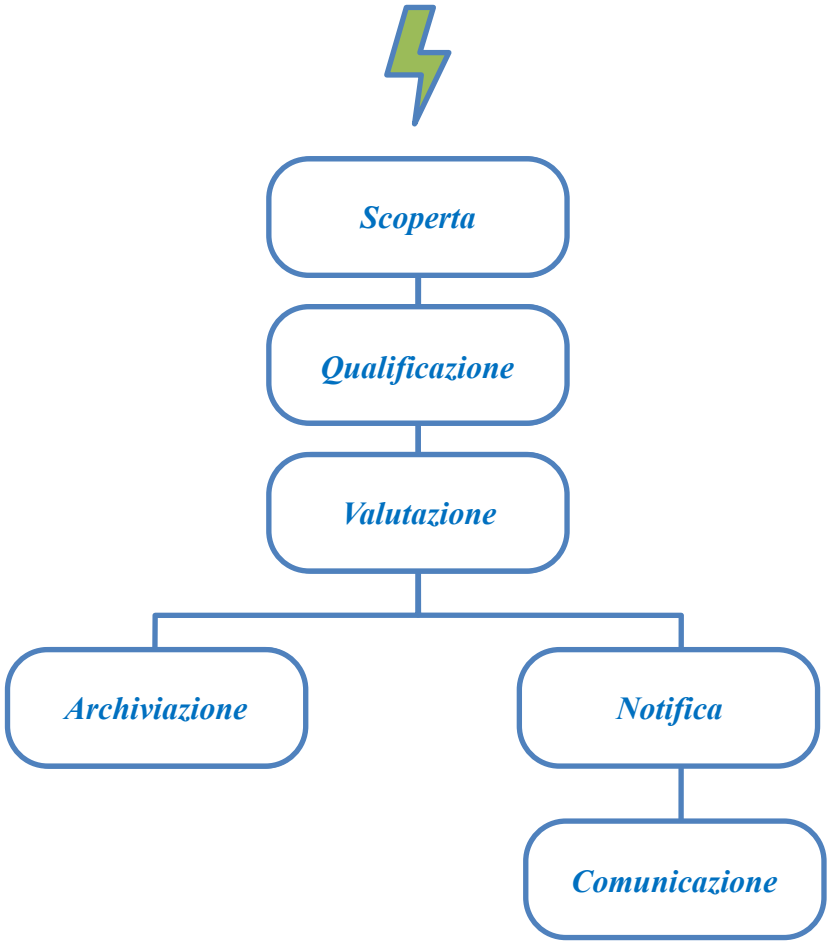
Codice	Significato
N	Non attivabile
R	Attivabile su richiesta
P	É definita una procedura specifica di valutazione
A	Attivabile direttamente dall'interessato tramite strumenti informatizzati

NOTIFICA DELLE VIOLAZIONI

"Data Breach notification"



72 ore



Registro attività di trattamento (Titolare)

Trattamenti					Dati Personali									
ID	Nome	Titolare (Contitolare)	Finalità	Interessati (Categorie)	ID	Dato / Categoria	Tipo	Destinatari	Trasferimento Paese terzo / Criterio	Periodo di Conservazione	Archivi fisici			
											ID	Archivio	C/I	Livello di Sicurezza (richiesto)
TRT1	Gestione clienti	Titolare: Azienda XYZ SpA	Finalità amministrative e contabili	Clienti	PII1	Contatti cliente	Norm.			Durata del rapporto contrattuale	DB1	FileSystem	I	Basso
TRT2	Gestione fornitori	Titolare: Azienda XYZ SpA		Fornitori	PII2	Contatti fornitore	Norm.			Durata del rapporto contrattuale	DB1	FileSystem	I	Basso
TRT3	Gestione Trouble tickets	Titolare: Azienda XYZ SpA		Clienti	PII1	Contatti cliente	Norm.				DB1	FileSystem	I	Alto
					PII3	Utilizzatori finali	Norm.				DB1	FileSystem	I	Medio
TRT4	Trattamento Dati Contabilità	Titolare: Azienda XYZ SpA		Clienti/ Fornitori/ Dipendenti	PII4	Dati contabilità	Norm.			10 anni	DB1	FileSystem	I	Medio
TRT5	Gestione Ordini Clienti	Titolare: Azienda XYZ SpA		Clienti	PII1	Contatti cliente	Norm.				DB1	FileSystem	I	Medio
TRT6	Registrazione visitatori	Titolare: Azienda XYZ SpA		Visitatori	PII5	Registro visitatori	Norm.			1 sett.	DOC1	Registro visitatori	C	Basso
TRT7	Tr. Dispositivi personali	Titolare: Azienda XYZ SpA		Dipendenti	PII6	Assegnazione	Norm.				DB1	FileSystem	I	Basso
TRT8	Tr. Viaggio	Titolare: Azienda XYZ SpA		Dipendenti	PII7	Dati anagrafici	Norm.				DOC2	Fatture tel.	C	Medio
TRT9	Tr. Note spese	Titolare: Azienda XYZ SpA		Dipendenti	PII9	Note spese	Norm.				DOC4	Doc. Note spese e giustificativi	C	Basso
TRT10	Tr. Parco auto	Titolare: Azienda XYZ SpA		Dipendenti	PII10	Dati anagrafici	Norm.				DOC5	Doc. parco auto	C	Basso
TRT11	Tr. Dati e-mail	Titolare: Azienda XYZ SpA		Dipendenti	PII11	Dati e-mail			- Giappone /		DB2	e-mail	I	Medio