Privacy Impact Assessment PIA

Versione Aprile 2018

Il Decreto Legislativo 30 giugno 2003 n°196, codice in materia di protezione dei dati personali, è rivolto a garantire "che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".
A tale scopo la legge istituisce una Autorità garante e definisce, con riferimento al trattamento dei dati, i soggetti - "interessato", "titolare", "responsabile" e "incaricato" - che a vario titolo possono essere parte in causa nel trattamento medesimo.
Rimandando alle definizioni per l'illustrazione dei principali aspetti della legge, qui intendiamo fornire chiarimenti e istruzioni operative ai responsabili e agli incaricati al trattamento dei dati.
Recepisce anche le modifiche e integrazioni introdotte il 4 maggio 2016 è stato pubblicato nella **Gazzetta Ufficiale dell'Unione Europea** il nuovo **Regolamento (UE) 2016/679** del Parlamento Europeo e del Consiglio *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione ditali dati e che abroga la direttiva 95/46/CE* (regolamento generale sulla protezione dei dati) **da cui era disceso il D.Lgs. 196/2003.**
Il presente documento integra la Guida all'applicazione del Regolamento UE 2016/679 in materia di protezione dei dati personali emessa dal Garante della privacy definita **GDPR** in inglese o **RGPD** in italiano.
La Guida traccia un **quadro generale delle principali innovazioni introdotte** dalla normativa e fornisce indicazioni utili sulle prassi da seguire e gli adempimenti da attuare per dare corretta applicazione alla normativa, già in vigore dal 24 maggio 2016 e che sarà pienamente efficace dal 25 maggio 2018.
Essenzialmente:

- il **Titolare del trattamento** nella 196 resta inalterato nel RPGD (GDPR -> data controller)
- il **Responsabile del trattamento** nella 196 resta inalterato nel RPGD (GDPR -> data processor)
- viene introdotto il **Responsabile protezione dei dati** nel RPGD (GDPR -> data protection officer **DPO**) che appare non ricorrere per Cassa Cooperativa
- **L'incaricato del trattamento** nel RPGD e ne GDPR viene generalizzato in chiunque agisca sollo la sua autorità o sotto quella del responsabile del trattamento
- **L'amministratore del sistema** della 196 viene di fatto convertito in **Responsabile del trattamento**

Nel documento si userà la notifica inglese (GDPR, DPO.....)
Inizia a integrare inoltre la normativa sulla sicurezza reti NIS2018/151 NIS attiva dal 10/5/18

	Nominativo	Firma	Data
Titolare del trattamento	Andrea Bottazzi		17/04/2018
Responsabile del trattamento	Andrea Bottazzi		17/04/2018

Indice

1. Campo di applicazione

Il presente regolamento riguarda tutti i trattamenti di dati personali effettuati dalla CassaCoop inerenti i soci della cooperativa stessa.

2. Decreto Legislativo 30 giugno 2003 n° 196 integrato dal UE 2016/679 GDPR

Gli aspetti più rilevanti del Decreto Legislativo 30 giugno 2003 n°196 e integrato dal UE 2016/679 e dalle integrazioni del Garante sono:

Principi di base:

1. La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale.
2. dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o residenza.
3. un obiettivo è armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri.
4. Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo.
5. La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo.
6. È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.
7. Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio. Non dovrebbero rientrare nell'ambito di applicazione del presente regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine.
8. Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.
9. I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore. **DI NORMA LA CASSA NON TRATTA DATI DI MINORI**.

Quadro normativo vigente

• il Regolamento n. 679/2016, Regolamento Generale sulla Protezione dei Dati (RGPD), entrato in vigore il 24 maggio scorso, **applicabile dal 24 maggio 2018**, che aggiorna e integra la Direttiva 95/46/CE;
• il Regolamento n. 910/2014, Regolamento Electronic Identification Authentication and Signature (Regolamento EIDAS), entrato in vigore il 17 settembre 2014, applicabile dallo scorso primo luglio, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, che sostituisce il quadro normativo definito dalla Direttiva Europea 1999/93/EC;
*la Direttiva n. 680/2016, entrata in vigore il 24 maggio scorso, sul trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, che abroga la decisione quadro 2008/977/GAI del Consiglio;
• la Direttiva n. 1148/2016, Direttiva Network and Information Security (Direttiva NIS), entrata in vigore l'8 agosto scorso, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
Il Legislatore si è impegnato affinché i contenuti delle succitate disposizioni siano efficaci, funzionino nella pratica e perdurino per almeno una generazione.
Sono norme complesse, che richiedono spesso la consulenza di esperti, non solo in questioni giuridiche ma delle complesse problematiche di compliance.
Il Regolamento GPD ed il Regolamento EIDAS, normativamente parlando, non necessitano di recepimento.
Il Regolamento EIDAS è già applicabile, il RGPD lo sarà dal 25 maggio 2018.
la Direttiva NIS e la Direttiva 680/2016 ora 2018/151 sarà in vigore dal **10 Maggio 2018**.

Modalità del trattamento e requisiti dei dati

I dati personali oggetto di trattamento sono:

a. Trattati in modo **lecito** e secondo **correttezza**; raccolti in maniera **trasparente** con comunicazioni chiare e comprensibili
b. Raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini esclusivamente compatibili con tali scopi;<<**limitazione della finalità**>>
c. Esatti e, se necessario, aggiornati, devono essere adottate tutte le misure ragionevoli per cancellare o rettificare i dati inesatti per le finalità per cui sono raccolti <<**esattezza**>>
d. Adeguati , pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati <<**minimizzazione dei dati**>>;
e. Conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.<<**limitazione della conservazione**>>
f. Raccolti con il chiaro consenso dell'interessato, ove possibile in maniera documentabile
g. Il trattamento dovrebbe essere considerato lecito se è necessario nell'ambito di un contratto o ai fini della conclusione di un contratto
h. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato dovrebbe avere il diritto, in qualsiasi momento e gratuitamente, di opporsi a tale trattamento, sia con riguardo a quello iniziale o ulteriore, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Tale diritto dovrebbe essere esplicitamente portato all'attenzione dell'interessato e presentato chiaramente e separatamente da qualsiasi altra informazione.
i. La profilazione è soggetta alle norme del presente regolamento che disciplinano il trattamento dei dati personali, quali le basi giuridiche del trattamento o i principi di protezione dei dati.
j. Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità.
k. Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento deve valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale. il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura,la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in

considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento. <<**integrità e riservatezza**>>

l. Il titolare del trattamento è competente per il rispetto dei dati personali (cfr punti precedenti) e in grado di comprovarlo <<**responsabilizzazione o accountability**>>

Sono pertanto importanti le valutazioni quanto più precise del rischio integrata nei processi aziendali con

m. Analisi trattamenti

- Identificazione tipologia dati trattati e soggetti coinvolti
- Mappatura flussi dati
- Valutazione rischio per la privacy e speculare sicurezza dei dati
- Contromisure per mitigare o ridurre al massimo i rischi
- Design dei processi aziendali secondo norme ed efficaci nella valorizzazione dei dati aziendali

Conseguenze sono che per ogni operazione serve un supporto documentale adeguato su cui si possa procedere a controlli sulle operazioni

- Caratteristiche
- Motivazioni
- Autorizzazioni
- Chi ha effettuato l'azione
- Chi ha registrato
- Chi ha verificato

Ovviamente si raccomanda un adeguato sistema di monitoraggio per documentare quanto sopra

Si riporta un elenco delle banche dati considerate, con i dettagli del caso.

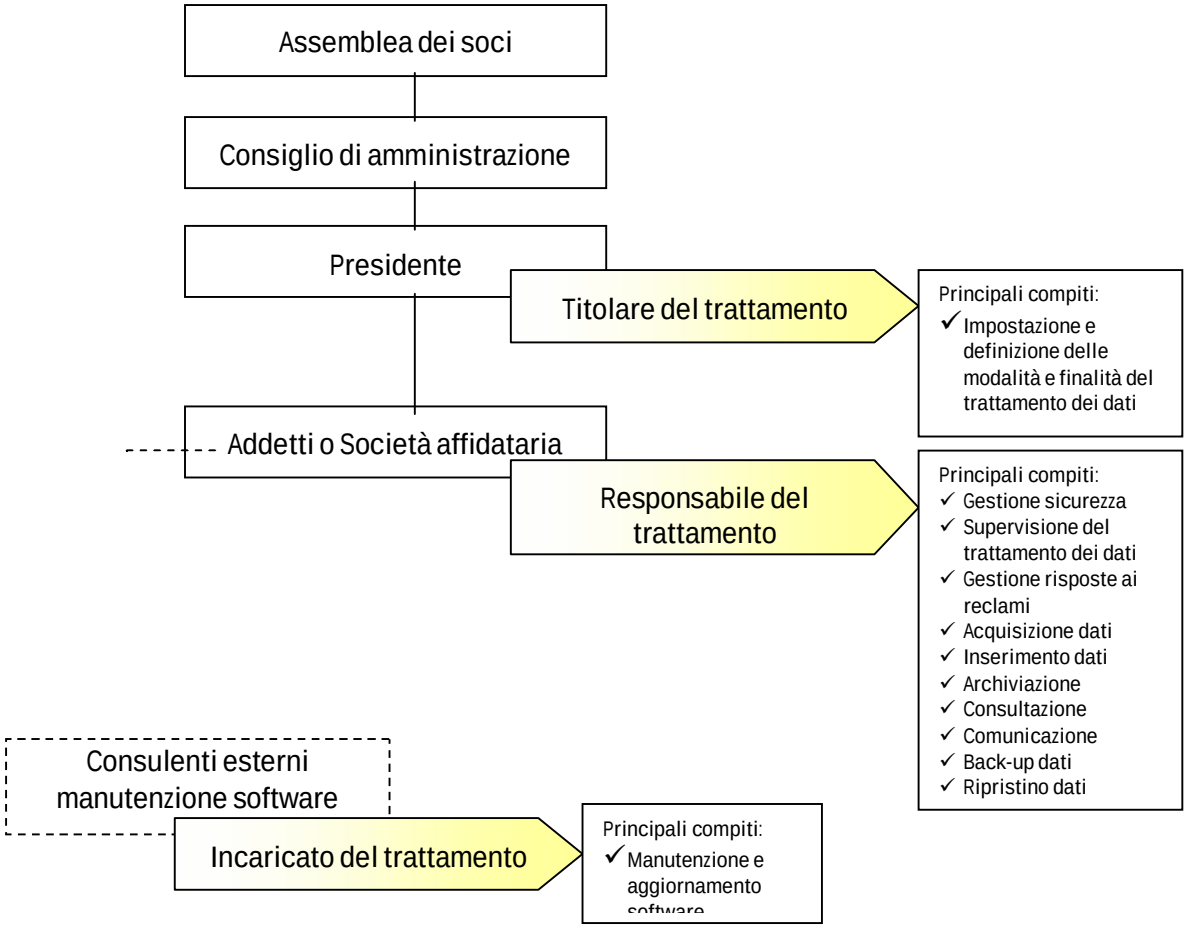
BANCA DATI	**ANAGRAFICA SOCI**
Categoria interessata	Tutti i dipendenti TPER che diventano soci della cooperativa
Dati	**Sensibili Sanitari:** Certificati medici cartacei **Giudiziari:** Nessuno **Personali:** Dati anagrafici clienti + coordinate bancarie ; mail e cellulari per comunicazioni urgenti sulle attività, dato ritenuto necessario per la sicurezza del cliente
Archivio (cartaceo / magnetico)	**Magnetico:** Software MIT (Soci) **Cartaceo:** Archivio CassaCoop
Finalità e modalità del trattamento	✓ Iscrizione alla cooperativa ✓ Comunicazioni con i soci ✓ Comunicazioni con enti esterni (Banca d'Italia, Finanza, ...) ✓ Gestione movimenti contabili soci ✓ Comunicazioni urgenti a tutela del socio, anche elettroniche
Nome del Responsabile del trattamento	Andrea Bottazzi
Incaricati del trattamento esterni	Circolo Coop Dozza, Mit, Aberas, Protovision (sistemi e HW), Sindaci e Revisori, Aruba, Legalmail, NETInsurance per cessioni quinto, Notai e Banche per surroghe mutui; Consiglieri

BANCA DATI	**CONTABILITA' CASSACOOP**
Categoria interessata	Tutti i dipendenti TPER che diventano soci della cooperativa
Dati	**Sensibili:** Nessuno **Giudiziari:** Nessuno **Personali:** Dati anagrafici clienti + coordinate bancarie ; mail e cellulari per comunicazioni urgenti sulle attività, dato ritenuto necessario per la sicurezza del cliente
Archivio (cartaceo / magnetico)	**Magnetico:** Software ABC **Cartaceo:** Archivio CassaCoop
Finalità e modalità del trattamento	Gestione movimenti contabili soci
Nome del Responsabile del trattamento	Andrea Bottazzi
Incaricati del trattamento	Circolo Coop Dozza, Mit, Aberas, Protovision (sistemi e HW), Sindaci e Revisori, Aruba, Legalmail, NETInsurance per cessioni quinto, Notai e Banche per surroghe mutui; Consiglieri

BANCA DATI	**ANAGRAFICA FORNITORI**
Categoria interessata	Tutti i fornitori della CassaCoop
Dati personali	**Sensibili:** Nessuno **Giudiziari:** Nessuno **Personali:** Dati anagrafici fornitori
Archivio (cartaceo / magnetico)	**Magnetico** : Software ABC **Cartaceo :** Archivio CassaCoop
Finalità e modalità del trattamento	Pagamento fornitori Registrazioni contabili e fiscali
Nome del Responsabile	Andrea Bottazzi
Incaricati del trattamento	Circolo Coop Dozza, Mit, Aberas, Protovision (sistemi e HW)

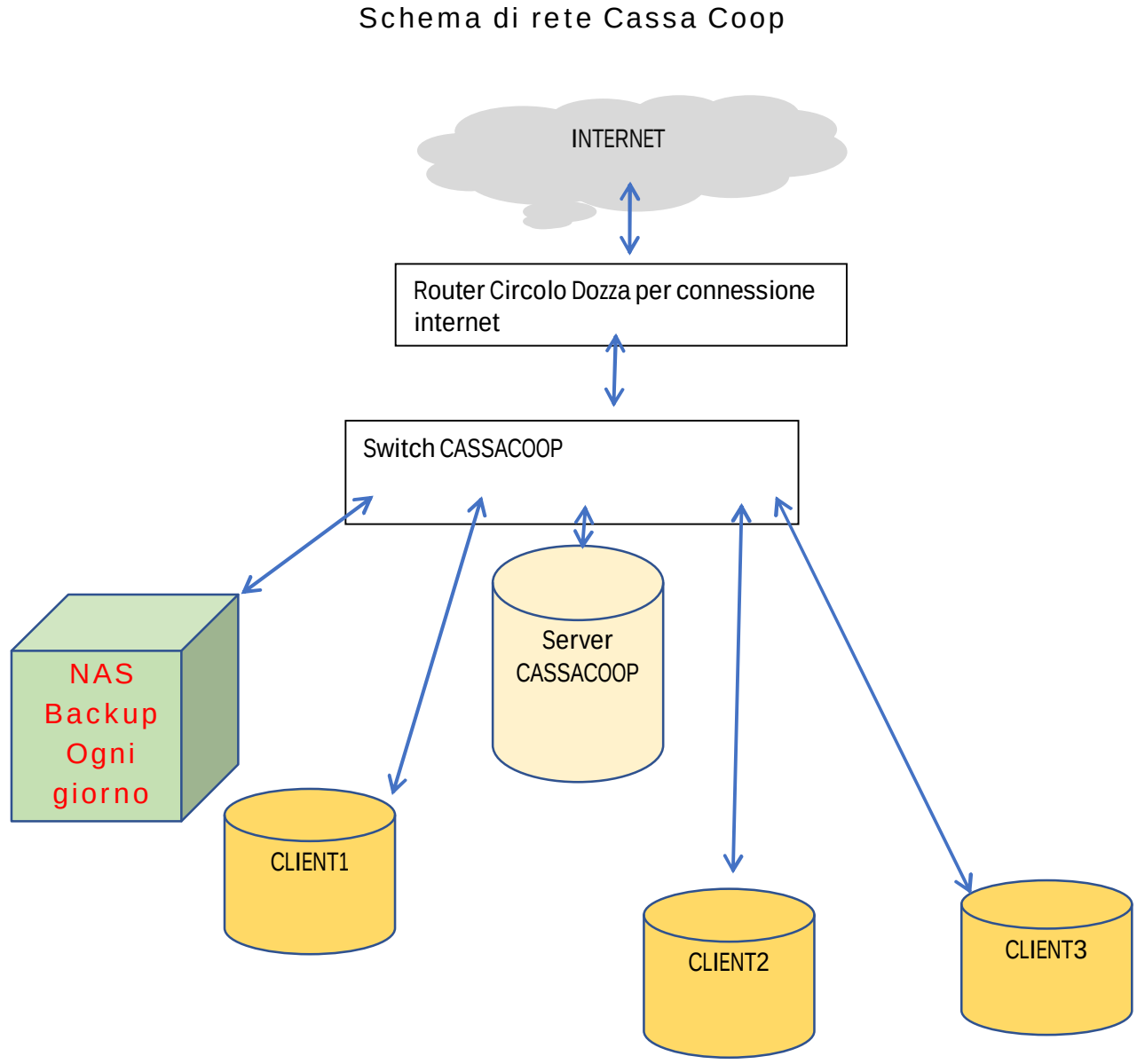
3. Responsabilità

Di seguito si riporta uno schema della struttura della Cassa Cooperativa in relazione alle responsabilità legate al trattamento dei dati.



4. Analisi dei rischi

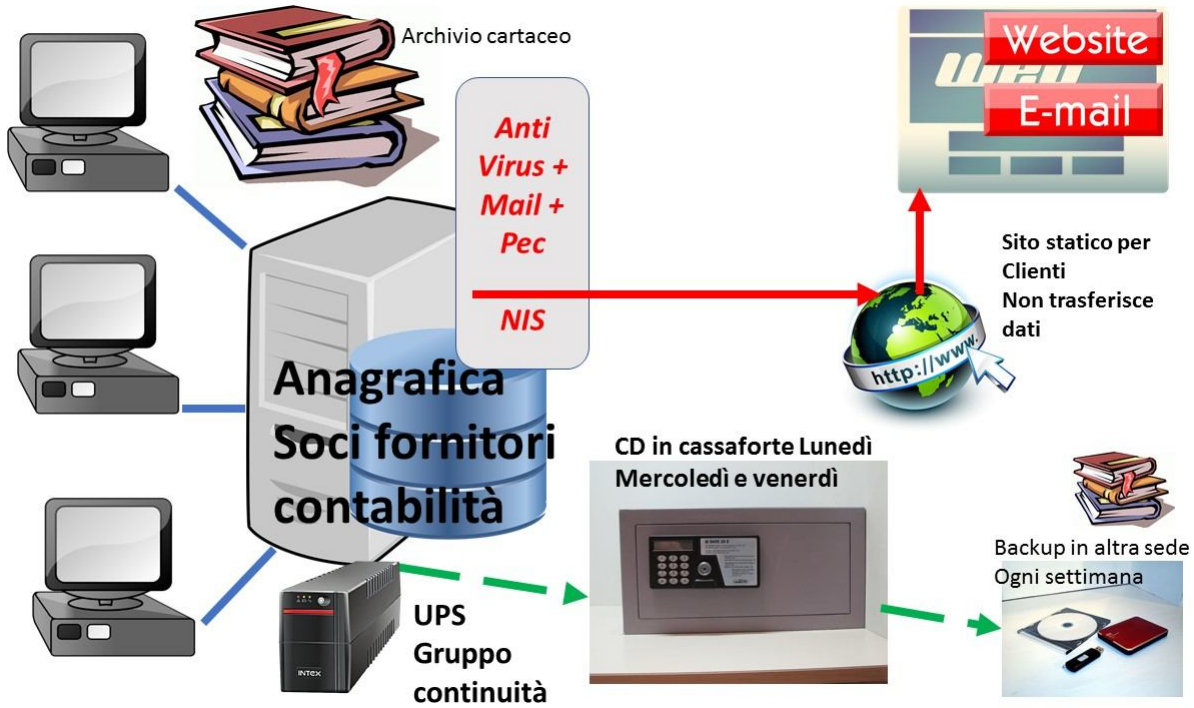
Schema di rete



SERVER CASSACOOP:
Macchina server con dischi mirrorati e con S.O. Windows server 2008 R2
Dischi in NAS per repository dati e backup
SW:
MIT (Gestionale finanziario) su Db FOX PRO
ABC (gestione contabilità) su Db FOX PRO
Office 2013
Entratel per comunicazione Agenzia Entrate
Antivirus NOB32

CLIENT1 -2- 3 CASSACOOP:
L'elaborazione dei dati avviene loggandosi in ***terminal server*** sul server CASSACCOOP che contiene anche i dati
Macchina ***Windows***
SW:
Office
Antivirus NOB32

Tutte le macchine sono protette da una telecamera di videosorveglianza all'ingresso dell'area di proprietà e gestione del circolo Dozza



Per ogni archivio sono qui riportate le analisi dei possibili rischi.

NOME DELL'ARCHIVIO:	**DATABASE ANAGRAFICA SOCI**
Tipologia archivio:	DB stand alone
Ubicazione fisica:	Server presso locale CassaCoop
Metodo di accesso:	Attraverso Server su cui è installato il programma dotato di accesso mediante nome utente e password personali
Trattamento finalità:	✓ Iscrizione alla cooperativa ✓ Comunicazioni con i soci ✓ Comunicazioni con enti esterni (Banca d'Italia, Finanza, ...) ✓ Gestione movimenti contabili soci
Comunicazione/diffusione all'esterno:	Richiesta di dati da parte di enti esterni (Banca d'Italia, Finanza, ...)
ELEMENTI DI RISCHIO	**DESCRIZIONE RISCHIO**
Rischi connessi all'ubicazione fisica	Intrusione nei locali Incendi o altri eventi eccezionali (terremoti, ...)
Rischi connessi al metodo di accesso ai dati	Accesso non controllato ai dati
Rischi connessi alla comunicazione e diffusione	Legate alle modalità di comunicazione richieste (cartacee, informatiche, ...)
Rischi connessi alle modalità di conservazione	Smagnetizzazione o guasto dei supporti informatizzati

NOME DELL'ARCHIVIO:	**ARCHIVIO ANAGRAFICA SOCI**
Tipologia archivio:	Cartaceo
Ubicazione fisica:	Armadi presso locale CassaCoop
Metodo di accesso:	Manuale
Trattamento finalità:	✓ Iscrizione alla cooperativa ✓ Comunicazioni con i soci ✓ Gestione movimenti contabili soci
Comunicazione/diffusione all'esterno:	Nessuno
ELEMENTI DI RISCHIO	**DESCRIZIONE RISCHIO**
Rischi connessi all'ubicazione fisica	Intrusione nei locali Incendi o altri eventi eccezionali (terremoti, ...)
Rischi connessi al metodo di accesso ai dati	Accesso non controllato all'archivio
Rischi connessi alla comunicazione e diffusione	Nessuno
Rischi connessi alle modalità di conservazione	Deterioramento dei supporti

NOME DELL'ARCHIVIO:	**CONTABILITA' CASSACOOP**
Tipologia archivio:	Software ABC
Ubicazione fisica:	Server presso locale CassaCoop
Metodo di accesso:	Attraverso Server su cui è installato il programma dotato di accesso mediante nome utente e password personali
Trattamento finalità:	Gestione movimenti contabili soci
Comunicazione/diffusione all'esterno:	Richiesta di dati da parte di enti esterni (Banca d'Italia, Finanza, ...)
ELEMENTI DI RISCHIO	**DESCRIZIONE RISCHIO**
Rischi connessi all'ubicazione fisica	Intrusione nei locali Incendi o altri eventi eccezionali (terremoti, ...)
Rischi connessi al metodo di accesso ai dati	Accesso non controllato ai dati
Rischi connessi alla comunicazione e diffusione	Legate alle modalità di comunicazione richieste (cartacee, informatiche, ...)
Rischi connessi alle modalità di conservazione	Smagnetizzazione o guasto dei supporti informatizzati

NOME DELL'ARCHIVIO:	**ARCHIVIO CONTABILITA' CASSACOOP**
Tipologia archivio:	Cartaceo
Ubicazione fisica:	Armadi presso locale CassaCoop
Metodo di accesso:	Manuale
Trattamento finalità:	Gestione movimenti contabili soci
Comunicazione/diffusione all'esterno:	Richiesta di dati da parte di enti esterni (Banca d'Italia, Finanza, ...)
ELEMENTI DI RISCHIO	**DESCRIZIONE RISCHIO**
Rischi connessi all'ubicazione fisica	Intrusione nei locali Incendi o altri eventi eccezionali (terremoti, ...)
Rischi connessi al metodo di accesso ai dati	Accesso non controllato all'archivio
Rischi connessi alla comunicazione e diffusione	Legate alle modalità di comunicazione richieste (cartacee, informatiche, ...)
Rischi connessi alle modalità di conservazione	Deterioramento dei supporti

NOME DELL'ARCHIVIO:	DATABASE ANAGRAFICA FORNITORI
Tipologia archivio:	DB stand alone
Ubicazione fisica:	Server presso locale CassaCoop
Metodo di accesso:	Attraverso Server su cui è installato il programma dotato di accesso mediante nome utente e password personali
Trattamento finalità:	✓ Ordini ✓ Registrazione fatture ✓ Pagamento fatture
Comunicazione/diffusione all'esterno:	Nessuno
ELEMENTI DI RISCHIO	**DESCRIZIONE RISCHIO**
Rischi connessi all'ubicazione fisica	Intrusione nei locali Incendi o altri eventi eccezionali (terremoti, ...)
Rischi connessi al metodo di accesso ai dati	Accesso non controllato ai dati
Rischi connessi alla comunicazione e diffusione	Nessuno
Rischi connessi alle modalità di conservazione	Smagnetizzazione o guasto dei supporti informatizzati

NOME DELL'ARCHIVIO:	ARCHIVIO FORNITORI
Tipologia archivio:	Cartaceo
Ubicazione fisica:	Armadi presso locale CassaCoop
Metodo di accesso:	Manuale
Trattamento finalità:	✓ Ordini ✓ Registrazione fatture ✓ Pagamento fatture
Comunicazione/diffusione all'esterno:	Nessuno
ELEMENTI DI RISCHIO	**DESCRIZIONE RISCHIO**
Rischi connessi all'ubicazione fisica	Intrusione nei locali Incendi o altri eventi eccezionali (terremoti, ...)
Rischi connessi al metodo di accesso ai dati	Accesso non controllato all'archivio
Rischi connessi alla comunicazione e diffusione	Nessuno
Rischi connessi alle modalità di conservazione	Deterioramento dei supporti

5. Misure di sicurezza

Si riportano per ogni archivio le misure di sicurezza adottate per garantire la privacy dei dati trattati.

NOME DELL'ARCHIVIO:	**DATABASE ANAGRAFICA SOCI**
Tipologia archivio:	DB stand alone
Ubicazione fisica:	Server presso locale CassaCoop
Sicurezze fisiche adottate	✓ Ingresso controllato al locale (telecamera Circolo Dozza nel corridoio) ✓ Sistemi di controllo accessi ✓ Custodia in luoghi non accessibili di copie di backup ✓ Dispositivi antincendio ✓ Continuità dell'alimentazione elettrica
Sicurezze logiche adottate	✓ Identificazione degli incaricati ✓ Controllo accesso Server mediante password personali ✓ Back-up periodico scaricati il Lun.Mer.Ven. E trasferiti presso sede legale ✓ Controlli aggiornati antivirus (***NOD32 , Kasperky***)
Sicurezze organizzative	✓ Definizione di linee guida di sicurezza per il trattamento dei dati ✓ Definizione delle responsabilità nel trattamento dei dati per le attività esternalizzate

NOME DELL'ARCHIVIO:	**ARCHIVIO ANAGRAFICA SOCI**
Tipologia archivio:	Cartaceo
Ubicazione fisica:	Armadi presso locale CassaCoop
Sicurezze fisiche adottate	➢ Ingresso controllato al locale (telecamera Circolo Dozza nel corridoio) ➢ Sistemi di controllo accessi ➢ Registrazione degli accessi ➢ Custodia in armadi non accessibili al pubblico ➢ Dispositivi antincendio
Sicurezze logiche adottate	➢ Identificazione degli incaricati
Sicurezze organizzative	➢ Definizione di linee guida di sicurezza per il trattamento dei dati

NOME DELL'ARCHIVIO:	**CONTABILITA' CASSACOOP**
Tipologia archivio:	Software ABC
Ubicazione fisica:	Server presso locale CassaCoop
Sicurezze fisiche adottate	✓ Ingresso controllato al locale (telecamera Circolo Dozza nel corridoio) ✓ Sistemi di controllo accessi ✓ Custodia in luoghi non accessibili di copie di backup ✓ Dispositivi antincendio ✓ Continuità dell'alimentazione elettrica
Sicurezze logiche adottate	✓ Identificazione degli incaricati ✓ Controllo accesso Server mediante password personali ✓ Back-up periodico scaricati il Lun.Mer.Ven. E trasferiti presso sede legale ✓ Controlli aggiornati antivirus
Sicurezze organizzative	✓ Definizione di linee guida di sicurezza per il trattamento dei dati ✓ Definizione delle responsabilità nel trattamento dei dati per le attività esternalizzate

NOME DELL'ARCHIVIO:	ARCHIVIO CONTABILITA' CASSACOOP
Tipologia archivio:	Cartaceo
Ubicazione fisica:	Armadi presso locale CassaCoop
Sicurezze fisiche adottate	➢ Ingresso controllato al locale ➢ Sistemi di controllo accessi ➢ Registrazione degli accessi ➢ Custodia in armadi non accessibili al pubblico ➢ Dispositivi antincendio
Sicurezze logiche adottate	➢ Identificazione degli incaricati
Sicurezze organizzative	➢ Definizione di linee guida di sicurezza per il trattamento dei dati

NOME DELL'ARCHIVIO:	DATABASE FORNITORI
Tipologia archivio:	DB stand alone
Ubicazione fisica:	Server presso locale CassaCoop
Sicurezze fisiche adottate	✓ Ingresso controllato al locale ✓ Sistemi di controllo accessi ✓ Custodia in luoghi non accessibili di copie di backup ✓ Dispositivi antincendio ✓ Continuità dell'alimentazione elettrica
Sicurezze logiche adottate	✓ Identificazione degli incaricati ✓ Controllo accesso Server mediante password personali ✓ Back-up periodico ✓ Controlli aggiornati antivirus
Sicurezze organizzative	✓ Definizione di linee guida di sicurezza per il trattamento dei dati ✓ Definizione delle responsabilità nel trattamento dei dati per le attività esternalizzate

NOME DELL'ARCHIVIO:	ARCHIVIO FORNITORI
Tipologia archivio:	Cartaceo
Ubicazione fisica:	Armadi presso locale CassaCoop
Sicurezze fisiche adottate	➢ Ingresso controllato al locale ➢ Sistemi di controllo accessi ➢ Registrazione degli accessi ➢ Custodia in armadi non accessibili al pubblico ➢ Dispositivi antincendio
Sicurezze logiche adottate	➢ Identificazione degli incaricati
Sicurezze organizzative	➢ Definizione di linee guida di sicurezza per il trattamento dei dati

6. Linee guida per il trattamento dei dati

6.1. Generalità

I dati personali acquisiti devono essere trattati in modo lecito e corretto. Inoltre devono essere mantenuti esatti, completi, veritieri e sempre pertinenti alle finalità per le quali vengono trattati.

6.1.1. Raccolta dell'informativa - consenso

L'atto di informativa - consenso deve essere raccolto in tutti i casi in cui si acquisiscano dati personali.
Il consenso è manifestato in forma scritta.
I soggetti dei quali si trattano i dati personali sono i soci della CassaCoop.

Il modulo relativo all'informativa ed alla raccolta del consenso è in allegato al presente documento.
In ogni caso si è ritenuto più sicuro e prioritario per comunicazioni urgenti acquisire dai clienti soci cellulari e mail ove esistenti, pur senza renderlo vincolante.
Detti dati sono utilizzati SOLO ed ESCLUSIVAMENTE per chiamate di emergenza relativamente ai servizi della Cassa. E saranno cancellati un anno dopo la chiusura del rapporto.

6.1.2. Divieto di comunicazione o diffusione

Gli incaricati devono evitare che i dati personali acquisiti siano comunicati a soggetti diversi da quelli indicati nell'atto di informativa e utilizzati per finalità diverse da quelle per le quali sono stati acquisiti.
Devono altresì astenersi dal diffondere i dati personali.
Gli incaricati dovranno restituire integralmente i dati personali al Responsabile del trattamento, in seguito all'eventuale cessazione del rapporto di lavoro in essere, con espresso divieto di conservarli, duplicarli, comunicarli o diffonderli.

6.1.3. Norme di sicurezza

Secondo la legge i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
Gli incaricati dovranno cancellare i dati personali, in conformità alle istruzioni impartite dal titolare e/o responsabili, in caso di cessazione del trattamento o qualora siano esauriti gli scopi per i quali gli stessi sono stati raccolti o successivamente trattati.

6.1.4. Trattamenti con strumenti elettronici

Negli archivi informatici vengono conservati dati personali, il cui accesso è consentito solo tramite applicativo protetto tramite l'uso di una password personale.
Per garantirne il corretto funzionamento, occorre evitare il salvataggio di documenti contenenti dati personali in locale. Ogni incaricato deve comunque astenersi dall'accesso e dal trattamento dei dati che non siano strettamente necessari per il proprio lavoro. Ogni piattaforma elaborativa viene utilizzata con i livelli di sicurezza possibili sia a livello di sistema operativo che di applicativo.
La password può essere sostituita da ogni incaricato di propria iniziativa a meno che ciò non sia tecnicamente irrealizzabile. Gli incaricati provvedono ad aggiornare la password ogni tre mesi.
La password deve essere custodita in modo da garantirne la conoscenza esclusivamente da parte dell'incaricato.
Si consiglia di bloccare la postazione e/o uscire dagli applicativi in tutti i casi di significativo allontanamento dalla postazione di lavoro, e di svuotare quotidianamente il "cestino" di Windows (o analoghi).
E' vietato l'utilizzo di software non autorizzato dalla CassaCoop.
Gli elaboratori sono protetti da antivirus, che viene aggiornato automaticamente all'accensione.
Gli addetti gestiscono l'attività di backup e ripristino dei dati effettuando una copia dei dati, con frequenza giornaliera,che viene custodita nella cassaforte presso il locale della CassaCoop. In caso di necessità l'addetto garantisce il ripristino dei dati nel minor tempo possibile e generalmente in un giorno.

6.1.5. Regole per la gestione degli archivi cartacei

Negli archivi cartacei sono conservati dati personali.
In considerazione di ciò:

- ✓ È obbligatorio conservare i dati solo nei predetti archivi, evitando dunque di collocare i documenti che li contengono in luoghi diversi, o di lasciarli fuori dagli archivi stessi. In particolare non è consentito lasciare le pratiche contenenti dati personali, specie se sensibili, sulla scrivania o comunque a portata di mano se non per il tempo necessario all'effettivo utilizzo, al termine del quale i documenti devono essere riposti;
- ✓ ogni incaricato deve riporre i documenti contenenti i dati personali negli archivi, al termine delle operazioni affidate (ad esempio, al termine della giornata); allo stesso tempo, nel corso della giornata, i documenti –specie se contenenti dati sensibili- devono essere riposti o negli armadi o nei cassetti, purché chiusi, in ogni caso di allontanamento dell'incaricato dal proprio posto di lavoro;

- ✓ non sono ammessi accessi agli archivi cartacei fuori orario di lavoro se non da soggetti incaricati del trattamento.

Le regole per il materiale cartaceo appena descritte valgono anche per la conservazione dei dischi, che contengano, ovviamente, dati personali.

In particolare:

- ✓ gli "scarti di archivio": gli scarti di archivio, ossia il periodico smaltimento di materiale cartaceo o dischi o altri supporti precedentemente conservati, se riferito anche a dati personali, deve essere effettuato con alcune cautele. Occorre evitare che le informazioni personali possano essere utilizzate da persone non legittimate. A tal fine occorre aver cura, ad esempio, che:
  - ✓ i documenti vengano inseriti in contenitori chiusi (buste, scatoloni, etc.) senza specifiche indicazioni del contenuto;
  - ✓ i contenitori vengano introdotti direttamente nei cassonetti, e non lasciati a lato, ovvero smaltiti in altro modo egualmente "sicuro";
  - ✓ prima dello smaltimento, i documenti non vengano depositati, senza controllo, dentro o fuori i locali della CassaCoop.
  - ✓ I documenti contenenti dati personali vengono prima dello smaltimento distrutti in apposito distruggidocumenti Fellowes P500 sito presso la segreteria del Circolo Dozza.
- ✓ il riutilizzo dei supporti di memorizzazione: i supporti sui quali vengano anche occasionalmente "salvati" dati sensibili **non** possono essere riutilizzati
- ✓ Formazione

Tutti gli incaricati vengono informati dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi e dei contenuti della disciplina sulla protezione dei dati personali attraverso la diffusione del presente documento ed attraverso attività formative periodiche.

Inoltre sono programmate attività di formazione specifica in caso di assunzione, variazione di mansione o introduzione di nuove tecnologie/strumenti per il trattamento dei dati personali. Efettuato corso ai Consiglieri e agli addetti sulla nuova normativa regolamento UE 2016/679 e NIS 2018/151 al quale seguiranno aggiornamenti.

Il corso è durato 3 ore con sessione di domande e risposte

Il corso stesso è disponibile sulla rete della Cassa per ulteriori consultazioni

7. Aspetti principali della valutazione

✓ **informativa**

L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:

a. le finalità e le modalità del trattamento cui sono destinati i dati;
b. la natura obbligatoria o facoltativa del conferimento dei dati;
c. le conseguenze di un eventuale rifiuto di rispondere;
d. i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito dei dati medesimi;
e. i diritti di cui può usufruire;
f. gli estremi identificativi del titolare e, se designati, del rappresentante e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato, è indicato tale responsabile.

✓ **consenso**

1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.
2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all' articolo 13.
4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

✓ **divieti di comunicazione e diffusione**

1. La comunicazione e la diffusione sono vietate, oltre che in caso di divieto disposto dal Garante o dall' autorità giudiziaria:
   a. in riferimento a dati personali dei quali è stata ordinata la cancellazione ovvero quando è decorso il periodo di tempo indicato nell'articolo 11, comma 1, lettera e);
   b. per finalità diverse da quelle indicate nella notificazione del trattamento, ove prescritta.

✓ **notifica del trattamento**

non ricorre notifica al garante **non** trattando dati genetici, giudiziari, biometrici, di localizzazione, di telemarketing e di nessuna delle categorie indicate dal Garante,

✓ **obblighi di sicurezza**

I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distribuzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità delle raccolta.

✓ **Trattamenti con strumenti elettronici**

Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
   a. autenticazione informatica;
   b. adozione di procedure di gestione delle credenziali di autentificazione;
   c. utilizzazione di un sistema di autorizzazione;
   d. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
   e. protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
   f. adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
   g. tenuta di un aggiornamento documentato programmatico sulla sicurezza;
   h. adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

✓ **Trattamenti senza l'ausilio di strumenti elettronici**

Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
   a. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
   b. previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
   c. previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

.....

I dati personali acquisiti devono essere trattati in modo lecito e corretto. Inoltre devono essere mantenuti esatti, completi, veritieri e sempre pertinenti alle finalità per le quali vengono trattati.

8. Analisi dei rischi, delle risorse da proteggere , minacce e contromisure

L'analisi dei rischi consente di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo e avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.

L'analisi dei rischi consiste nella:

- individuazione di tutte le risorse del patrimonio informativo;
- identificazione delle minacce a cui tali risorse sono sottoposte;
- identificazione delle vulnerabilità;
- definizione delle relative contromisure.

INDIVIDUAZIONE DELLE RISORSE DA PROTEGGERE

Le risorse da proteggere sono:

- ✓ elenco clienti e fornitori;
- ✓ dati relativi al personale dipendente;
- ✓ dati/informazioni;
- ✓ documenti cartacei;
- ✓ hardware;
- ✓ software;
- ✓ apparecchiature di comunicazione;

INDIVIDUAZIONE DELLE MINACCE

Nella tabella seguente sono elencati gli eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse .

Terremoto ed eventi ambientali (pioggia, fulmini, inondazioni)
Danno di tipo ambientale, serietà gravissima, probabilità bassa, edifici stabili in area poco sismica

Atti di guerra e terrorismo
Danno di tipo deliberato e accidentale, serietà gravissima, probabilità bassa, edifici stabili in area politicamente stabile

Fuoco e incendio
Danno di tipo deliberato e accidentale, serietà gravissima, probabilità bassa, edifici protetti con estintori, vicinanza ai vigili del fuoco

Danni volontari, errori operativi voluti o meno
Danno di tipo deliberato e accidentale, serietà gravissima, probabilità bassa, contromisure quali formazione, procedure condivise, sede ben gestita con portineria

Furto
Danno di tipo deliberato e accidentale, serietà gravissima, probabilità bassa, contromisure quali formazione, procedure condivise, sede ben gestita con portineria

Interruzione di servizi (gas, riscaldamento, acqua, condizionamento)
Danno di tipo ambientale o accidentale, serietà media, probabilità bassa, edifici in area centrale, servizi di pronto intervento, possibilità di interrompere il servizio in presenza di gruppi di continuità

Interruzione linee di comunicazione dati
Danno di tipo ambientale o accidentale, serietà media, probabilità bassa, si considera a oggi marginale e non critica la necessità continua di rete dati, in futuro qualora diventi più critica la dipendenza si rivaluterà alla luce della diversa organizzazione

Guasti hardware (processori, dischi, alimentatori) , sofware, manutentivi
Danno di tipo accidentale, serietà media, probabilità bassa, si considera a oggi marginale e non critica la necessità continua di servizi, peraltro ulteriormente mitigabile con dischi ridondati, nas, san, buona gestione dei backup

Accessi alla rete indesiderati o malgestiti, software non gestito
Danno di tipo deliberato e accidentale, serietà normalmente bassa ma potenzialmente gravissima, probabilità bassa, contromisure quali formazione, procedure condivise, sede ben gestita con portineria, accessi alla rete obbligatori e controllati

Intercettazione, controllo e disturbo linee di comunicazione dati

Danno di tipo ambientale o accidentale, serietà alta, probabilità bassa, si considera a oggi marginale e non critica la necessità continua di rete dati, in futuro qualora diventi più critica la dipendenza si rivaluterà alla luce della diversa organizzazione e si dovranno prevedere procedure di controllo

INDIVIDUAZIONE DELLE CONTROMISURE

Le contromisure individuano le azioni che si propongono al fine di annullare o di limitare le vulnerabilità e di contrastare le minacce; esse sono classificabili nelle seguenti tre categorie:

1. contromisure di carattere fisico;
2. contromisure di carattere procedurale;
3. contromisure di carattere elettronico/informatico.

Contromisure di carattere fisico

le apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati personali o sensibili/giudiziari e apparecchiature di telecomunicazione, dispositivi di copia) e gli archivi cartacei contenenti dati personali o sensibili/giudiziari sono situati in locali ad accesso controllato;
i locali ad accesso controllato sono all'interno di aree sotto controllo xxx ;
i responsabili dei trattamenti sono indicati;
i locali ad accesso controllato sono chiusi e le chiavi sono di esclusivo utilizzo degli incaricati e responsabili;
l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area aziendale telecontrollata e con guardiania;
i locali sono provvisti di estintore;
le misure di cui sopra sono attive.

Contromisure di carattere procedurale

l'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate, in area telecontrollata e con guardiania;
i visitatori occasionali della aree ad accesso controllato sono accompagnati da un incaricato;
l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'Incaricato del trattamento di tali dati;
i documenti cartacei riservati, accessibili solo ai dipendenti della società Titolare dei dati sono conservati negli uffici stessi;

Inoltre, per il trattamento dei soli dati cartacei sono adottate le seguenti disposizioni:

- ✓ si accede ai soli dati strettamente necessari allo svolgimento delle proprie mansioni;
- ✓ si utilizzano archivi con accesso selezionato;
- ✓ atti e documenti devono essere restituiti al termine delle operazioni;
- ✓ è fatto divieto di fotocopiare/scannerizzare documenti senza l'autorizzazione del Responsabile del trattamento;
- ✓ è fatto divieto di esportare documenti o copie dei medesimi all'esterno della società senza l'autorizzazione del Responsabile del trattamento, tale divieto si estende anche all'esportazione telematica;
- ✓ il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti deve essere ridotto in minuti frammenti.

Contromisure di carattere elettronico/informatico

Dettagliate in seguito.

MINACCE A CUI SONO SOTTOPOSTE LE RISORSE HARDWARE

Le principali minacce alle risorse hardware sono:

i. malfunzionamenti dovuti a guasti;
j. malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;
k. malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica;
l. malfunzionamenti dovuti a sabotaggi, furti, intercettazioni (apparati di comunicazione).

MINACCE A CUI SONO SOTTOPOSTE LE RISORSE CONNESSE IN RETE

Le principali minacce alle risorse connesse in rete possono provenire dall'interno della società, dall'esterno o da una combinazione interno/esterno e sono relative:

m. all'utilizzo della LAN (local area network)/Intranet (interne);
n. ai punti di contatto con il mondo esterno attraverso Internet (esterne);
o. allo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interne/esterne).

MINACCE A CUI SONO SOTTOPOSTI I DATI TRATTATI

Le principali minacce ai dati trattati sono:

- ✓ accesso non autorizzato agli archivi contenenti le informazioni riservate (visione,modifica, cancellazione, esportazione) da parte di utenti interni e/o esterni;
- ✓ modifiche accidentali (errori, disattenzioni) agli archivi da parte di utenti autorizzati.

MINACCE A CUI SONO SOTTOPOSTI I SUPPORTI DI MEMORIZZAZIONE

Le principali minacce ai supporti di memorizzazione sono:

- ✓ distruzione e/o alterazione a causa di eventi naturali;
- ✓ imperizia degli utilizzatori;
- ✓ sabotaggio;
- ✓ deterioramento nel tempo (invecchiamento dei supporti);
- ✓ difetti di costruzione del supporto di memorizzazione che ne riducono la vita media;
- ✓ l'evoluzione tecnologica del mercato che rende in breve tempo obsoleti alcuni tipi di supporti.

Norme di sicurezza

Secondo la legge i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
Gli incaricati dovranno cancellare i dati personali, in conformità alle istruzioni impartite dal titolare e/o dai responsabili, in caso di cessazione del trattamento o qualora siano esauriti gli scopi per i quali gli stessi sono stati raccolti o successivamente trattati.
Ad ogni codice identificativo/password corrisponde un profilo che consente a ciascun incaricato di accedere ai dati necessari allo svolgimento dei propri compiti.
Le policy consentono di accedere a sistemi diversi o aree dati diverse gestite dall'amministrazione dei dati.
La password può essere sostituita da ogni incaricato di propria iniziativa a meno che ciò non sia tecnicamente irrealizzabile.
La password deve essere custodita in modo da garantirne la conoscenza esclusivamente da parte dell'incaricato.
È obbligatorio bloccare la postazione di lavoro in tutti i casi di significativo allontanamento dalla postazione di lavoro (dopo 10 minuti di inutilizzo lo screen saver automatico bloccherà la sessione).
Ogni piattaforma elaborativa viene utilizzata con i livelli di sicurezza possibili sia a livello di sistema operativo che di applicativo.
Uno stesso codice identificativo non può essere assegnato a persone diverse; i codici identificativi personali sono assegnati e gestiti dai Sistemi Informativi e Sviluppo Tecnologico in modo che ne sia prevista la disattivazione in caso di perdita dei requisiti che consentivano l'accesso all'elaboratore o in caso di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi; inoltre i Sistemi Informativi e Sviluppo Tecnologico effettuano un ulteriore controllo annuale sui codici identificativi per verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
Tutte le norme evidenziate sono volte alla protezione dei dati aziendali.
Oltre ai sistemi di protezione dei dati "standard" solo con la formazione del personale e la regolamentazione si possono cercare di evitare fughe di notizie/dati.
Per evitare occultamenti le policy di accesso (quindi di scrittura e cancellazione dei dati) devono essere rigorose.
Nessuna policy per quanto ben applicata può proteggere al 100%

Possibili opzioni per tutelare maggiormente i dati aziendali:

d. Impedire copie in locale di specifici set di dati
e. Impedire copie in locale su dispositivi rimovibili (dischi mobili, USB)
f. Impedire accesso con computer aziendali a reti wireless e da reti wireless alla rete Cassa cooperativa
g. Impedire di inviare dati in determinati formati via mail
h. Impedire programmi di sharing di disco o memoria

In ogni caso per garantirne il corretto funzionamento, occorre evitare il salvataggio di documenti contenenti dati personali in locale. Ogni incaricato deve comunque astenersi dall'accesso e dal trattamento dei dati, specie se sensibili, che non siano strettamente necessari per il proprio lavoro.
Ogni incaricato deve comunque astenersi da caricare dati non aziendali per non introdurre malware.
Ove è deficitaria la sicurezza fisica (aree condivise con altre aziende, sale comuni, armadi in aree aperte a dipendenti di altre società o al pubblico) occorre:

- Massimizzare la sicurezza fisica con armadi chiusi e allarmati
- Massimizzare la sicurezza logica degli apparati rendendoli accessibili solo agli amministratori
- Attivare monitoraggi su accessi e tentati accessi
- Bloccare chiavi fisiche di accesso (prese dati, console operative, porte usb o simili)

Le perdite occasionali di dati vanno prevenute con adeguate policy di backup.
Tutte le policy di ridondanza, che prevengono le perdite dati, dovrebbero essere adottate sui server critici
Periodici backup, su disco, nastro o apposite librerie o in rete consentono di evitare perdite dati operando dei restore, dati conservati in sede remota diversa dalla operativa.
Il ripristino, attraverso il restore, consente di recuperare i dati all'istante del salvataggio.
È buona norma testare il restore (su dati reali) almeno una volta l'anno e all'atto dell'installazione di nuovi dispositivi, nuovi software e nuove reti.
In caso di crash di una o più macchine è necessario avere in stand by o di rapidissimo approvvigionamento una macchina simile o aver predisposto l'installazione dei software su altre macchine con spazio disco e capacità sufficienti.

Elaboratori in rete e/o isolati

Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se

- ✓ autenticazione informatica;
- ✓ adozione di procedure di gestione delle credenziali di autentificazione;
- ✓ utilizzazione di un sistema di autorizzazione;
- ✓ aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- ✓ protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- ✓ adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- ✓ tenuta di un aggiornamento documentato programmatico sulla sicurezza e/o di PIA;

Negli archivi informatici vengono conservati dati personali .
Ogni incaricato possiede uno specifico codice identificativo ed una parola-chiave (o "password") per l'accesso ai dati personali.
Ogni incaricato deve comunque astenersi dall'accesso e dal trattamento dei dati, specie se sensibili, che non siano strettamente necessari per il proprio lavoro.
Ogni piattaforma elaborativa viene utilizzata con i livelli di sicurezza possibili sia a livello di sistema operativo che di applicativo.
E' vietato l'utilizzo di software non autorizzato dall'Azienda.
I dispositivi diversi dagli elaboratori, come i dispositivi di rete quali: router, firewall, modem non disponendo di interfaccia uomo macchina banale (tastiera + schermo) sono meno attaccabili.
In ogni caso hanno implementato anch'essi security di accesso e spesso sono posizionati in locali chiusi e/o allarmati.
Gli elaboratori sono protetti da antivirus, che viene aggiornato giornalmente: è necessario segnalare ai Sistemi Informativi e Sviluppo Tecnologico ogni eventuale disfunzione.
In caso di necessità i Sistemi Informativi e sviluppo tecnologico garantiscono il ripristino dei dati nel minor tempo possibile (max qualche giorno)

Sicurezza dati anti intrusione fisica e videosorveglianza

La sede Cassa Cooperativa non è protetta da un sistema di videosorveglianza proprio ma del gestore della sede.

La sede è protetta attraverso:

1. accesso agli uffici con riconoscimento , o chiave
2. sistemi di backup
3. gruppi di continuità
4. rete elettrica certificata
5. rete dati certificata
6. sistemi di rinfrescamento
7. riscaldamento
8. armadi chiusi e/o allarmati
9. porte esterne allarmate fuori dagli orari di ufficio

9. Piani di miglioramento a breve e medio periodo

A breve termine (2018)

Ottimizzare i backup

Analizzare l'evoluzione tecnologica del software studiando soluzioni moderne e ben mantenute

Fare una ripresa del corso privacy su

- **phishing**, tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.
- **Social engineering** attacchi che inducono le vittime a fare passi falsi che rendano possibile l'attacco informatico

A medio termine (2019)

Ottimizzare i backup strutturando un rapido disaster recovery su cloud
Strutturare sul sito una area riservata per ogni cliente che consenta di superare l'invio degli estratti conto attraverso mail e renda disponibile il saldo, in sola lettura con credenziali personali , a cadenze mensili.
Controllo del solo invio verso il sito con certificati che non consentano l'accesso dal sito alla rete.
Integrazione con le basi dell'intrusion detection sul sito con test annuali
Tool di disconnessione di server e PC dalla rete dopo aver garantito i backup
Rendere disponibili on line i documenti di legge sulla normativa del credito

Analizzare l'evoluzione tecnologica del software studiando soluzioni moderne e ben mantenute

10. Allegati

Nomine responsabili trattamento dati interni con lettere di incarico
Consigliere del CDA Campnini Denis
Consigliere del CDA Vignoli Claudio
Consigliere del CDA Lodi Lamberto
Consigliere Vice Presidente del CDA Monterumisi Mara
Consigliere del CDA Bernardi Renata
Consigliere del CDA Bertocchi Roberto
Consigliere del CDA Cagossi Fabrizio
Consigliere del CDA Costa Annalisa
Consigliere del CDA Grimaldi Mariarosaria
Consigliere del CDA Poletti Emanuela
Consigliere del CDA Ramazzotti Dora
Consigliere del CDA Santitoro Nunzia
Consigliere del CDA Spina Cristoforo
Consigliere del CDA Zappitello Paola
Consigliere del CDA Zironi Giacomo

Modulo responsabili interni

Lettera di nomina a responsabile interno trattamento dati

Bologna data
Alla cortese attenzione di …..

Oggetto : nomina a responsabile interno del trattamento dati ai sensi e per gli effetti del DLgs 196/03 e del GDPR 2016/679 UE

Nella qualità di Responsabile del trattamento dei dati personali dei clienti di CassaCoop Dipendenti S.P. Mobilità Integrata E.R, nell'ambito della propria Struttura Organizzativa avrà la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni della normativa vigente nonché le istruzioni impartite dal titolare anche mediante comunicazioni ed ordini di servizio.

Lei ha il compito di adempiere a tutto quanto necessario per il rispetto delle vigenti disposizioni ed osservare scrupolosamente quanto previsto aziendalmente per la tutela della riservatezza rispetto al trattamento dei dati personali, in particolare con il compito di:

- Rispettare le misure di sicurezza aziendali e comunque almeno quelle previste dall'allegato B) del DLgs 196/03 e del GDPR 2016/679 UE
- Informare prontamente il Titolare di ogni questione rilevante ai fini della privacy
- Aver cura che ogni dato, elenco o banca dati oggetto del trattamento venga trattato per i soli fini per i quali è destinato
- Distruggere i dati personali alla cessazione del trattamento degli stessi, provvedendo alle formalità di legge e dandone comunicazione al Titolare, procedendo altresì all'aggiornamento dei dati e trattamenti
- Evadere tempestivamente i reclami degli interessati ai sensi dell'art.7 DLgs 196/03 e le eventuali istanze al Garante, dandone comunicazione al Titolare.
- Controllare l'andamento delle relazioni con gli utenti e/o i rischi connessi
- Curare il coordinamento di tutte le operazioni di trattamento dati
- Dare istruzioni per la corretta elaborazione dei dati personali

Nomine responsabili esterni di trattamento dati con lettere di incarico o con nota sul contratto

Aberas
Aruba
Legalmail
CoopDozza
Net Insurance
Net Insurance live
Commercialista Dott.ssa Magi Angelica
Sindaco Dott. Camellini Germano
Presidente del Collegio Sindacale Dott. Gamberini Riccardo
Commercialista Dott. Peloso Riccardo
Sindaco Dott.ssa Lipparini Francesca
Sindaco supplente Dott.Camellini Alberto
Sindaco supplente Dott.Molinari Davide
Mit
Protovision
Legacoop
Unicredit Spa (filiale via Ferrarese,85/a 40128 Bologna)
Banca di Bologna (filiale di Bologna Fiera District)
Emilbanca Credito Cooperativo (filiale 33 Business Park)
Bper Banca Spa (filiale via Venezian 5/a 40121 Bologna)
Società di revisione Aleph Auditing SRL
Notaio Avv.Rossi Angelelisa

Modulo responsabili esterni

CassaCoop Dipendenti S.P. Mobilità Integrata E.R., nella persona del Titolare dei trattamento dati Bottazzi Andrea e per gli effetti del DLgs 196/03, e del provvedimento del Garante per la protezione dei dati personali,

NOMINA E COSTITUISCE

_____ C.F. _____ e P.I. _____ quale responsabile esterno del trattamento dei dati personali, ai sensi e per gli effetti dell'art. 29 del D.Lgs 196/2003 (Codice in materia di protezione dei dati personali) e successive norme, esplicitamente il 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) .
Dovrà inoltre rispettare appieno le indicazioni della direttiva NIS (sicurezza reti) 2018/151 UE.

Nella qualità di Responsabile del trattamento dei dati personali dei clienti di CassaCoop Dipendenti S.P. Mobilità Integrata E.R, nell'ambito della propria Struttura Organizzativa avrà la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni della normativa vigente nonché le istruzioni impartite dal titolare anche mediante comunicazioni ed ordini di servizio.

Nello svolgimento delle sue attività dovrà:

1. svolgere il predetto incarico attenendosi ai criteri previsti dalla normativa vigente sulla tutela dei dati personali e sulle relative misure di sicurezza, riferiti al trattamento dei dati personali effettuato sia mediante archivi di tipo cartaceo o con strumenti diversi da quelli elettronici, sia con strumenti automatizzati elettronici;
2. definire per iscritto tutte le misure organizzative da predisporre in ottemperanza al D.Lgs. 196/2003 e successive norme, esplicitamente il 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) .
3. individuare, secondo idonee modalità, le figure professionali del trattamento dei dati, indicare i propri responsabili ed eventuali amministratori di sistema e indicare gli incaricati al trattamento di cui all'art. 30 del "Codice Privacy", dando loro istruzioni scritte;
4. impartire le disposizioni organizzative e operative e fornire agli incaricati le istruzioni per il corretto, lecito, pertinente e sicuro trattamento dei dati e vigilare affinché gli stessi incaricati al trattamento dei dati, di cui ai precedenti punti 2 e 3 si attengano alle procedure di volta in volta indicate specificatamente per iscritto;
5. procedere – ove necessario – al rilascio ed alla revoca delle autorizzazioni per l'accesso ai dati personali e vigilare affinché l'accesso ai dati da trattare da parte degli incaricati, sia limitato a quelli strettamente necessari allo svolgimento delle mansioni loro assegnate. In merito al mantenimento delle predette, il nominato Responsabile avrà il

compito di verificare la sussistenza delle condizioni che hanno determinato la loro emissione ed in difetto procedere alla loro revoca;

6. vigilare sulle modalità e procedure di trattamento e conservazione dei dati effettuate con supporto cartaceo o comunque in modo diverso da quello effettuato con strumenti elettronici o automatizzati. Al Responsabile sono altresì affidati il controllo, l'identificazione e la registrazione dei soggetti che hanno accesso agli archivi cartacei dopo l'orario degli uffici;
7. trasmettere le richieste degli interessati al titolare, ai fini dell'esercizio dei diritti dell'interessato, ai sensi degli artt. 7, 8, 9 e 10 del D.Lgs. 196/2003;

- stabilire le modalità di gestione e le forme di responsabilità relative a banche dati condivise da più Strutture Organizzative / Unità Operative / Settori / Staff o Progetti d'intesa con i relativi Responsabili;

9. proporre al Titolare del trattamento interno dei dati la nomina di soggetti esterni Responsabili del trattamento dati in riferimento all'affidamento agli stessi di determinate attività nell'ambito dei compiti della società;
10. intrattenere stretti rapporti di informazione e comunicazione con il titolare del trattamento e con gli altri collaboratori dello stesso.

_____

_____

Per Accettazione
Timbro e Firma

_____

Linee guida per il Responsabile del trattamento

Si evidenziano qui di seguito gli specifici adempimenti posti dalla legge a carico del Responsabile del trattamento da svolgere in coordinamento con il Referente Privacy.

p. Contribuire alla stesura del modello di valutazione dei rischi aziendali , al registro dei trattamenti per quanto di propria competenza e in caso comunicare come da GDPR eventuali data breach.

q. Individuare e designare responsabili, amministratori di sistema e addetti al trattamento dei dati personali; specificare l'ambito del trattamento consentito; impartire idonee istruzioni scritte circa le regole da rispettare nelle operazioni di trattamento svolte, nel rispetto del Codice e di quant'altro lo stesso Responsabile ritenga necessario; accertare che, nel caso di nuovi inserimenti di risorse, queste partecipino a corsi di formazione in materia di Privacy; pianificare incontri periodici per tutti i dipendenti al fine di aggiornare / adeguare le nozioni impartite.

r. Assicurare la qualità dei dati, le modalità di raccolta e conservazione degli stessi, nel rispetto di quanto indicato dal Codice Privacy, nonché vigilare sulla puntuale e corretta osservanza delle istruzioni impartite agli incaricati.

s. Garantire il rispetto dei diritti dell'interessato stabiliti dal Codice privacy.

t. Adottare le misure di sicurezza previste dal Codice Privacy, fermo restando che rientra comunque nei compiti del responsabile l'adozione di ulteriori e/o più restrittive misure rese necessarie dalla particolare tipologia di dati trattati e dalle modalità del trattamento.

u. Sottoporre al Titolare del trattamento l'eventuale nomina, a soggetti terzi, di "Responsabili esterni del trattamento dati" in riferimento all'affidamento di determinate attività, dandone informativa la Referente Privacy.

Nel caso di mancato rispetto delle istruzioni impartite dal Titolare, il Responsabile assume i rischi legati alla gestione dei dati personali e, conseguentemente, la responsabilità per eventuali trattamenti illeciti.

Informative privacy in uso,

Gentile cliente, con la presente comunicazione siamo ad informarla che i Suoi dati personali, anche sensibili, sono trattati per le seguenti finalità:

- Attività finanziarie proprie della Cassa;
- adempiere ad obblighi derivanti da leggi , norme e regolamenti comunitari
- far valere o difendere un diritto.

Il conferimento dei dati e il relativo trattamento sono obbligatori in relazione alle finalità indicate, ne consegue che l'eventuale rifiuto a fornire i dati per tali finalità potrà determinare l'impossibilità di CassaCoop Dipendenti S.P Mobilità Integrata E.R.- Società Cooperativa. a dare corso ai rapporti contrattuali medesimi e agli obblighi di legge.

I dati personali verranno trattati in forma cartacea ed informatizzata nel rispetto delle disposizioni di legge atte a garantire la riservatezza, la sicurezza e l'esattezza dei dati, l'aggiornamento e la pertinenza dei dati rispetto alle finalità dichiarate.

I dati di cui trattasi potranno essere comunicati ad altri enti/aziende per i servizi finanziari per i fini strettamente necessari per erogazioni/surroghe mutui e cessione del quinto.
Non è prevista in nessun altro caso la comunicazione dei dati personali ne in Italia, ne nella UE , ne tantomeno extra UE.
Il Titolare del trattamento è CassaCoop Dipendenti S.P Mobilità Integrata E.R.- Società Cooperativa, con sede in Bologna (BO),via Saliceto 3, e-mail info@cassacoopatc.it
Informativa completa e dettagliata, così come il testo integrale dell'art. 7, è disponibile sul sito internet di CassaCoop Dipendenti S.P Mobilità Integrata E.R.- Società Cooperativa: **http://www.cassacoopatc.it/cc/**

Consenso

Sottoscrivendo la presente dichiarazione prendo atto di potere conoscere ed esercitare i diritti previsti dall'art. 7 del D. Lgs. 30 giugno 2003 n. 196 e GDPR 2016/679rivolgendomi al Titolare o al Responsabile, in forma scritta, agli indirizzi sopra indicati. Il sottoscritto avendo preso visione della nota informativa esprime liberamente il consenso al trattamento e alla comunicazione dei propri dati personali, ivi inclusi i dati cosiddetti sensibili, da parte della società CASSA COOPERATIVA S.p.A. in relazione alle finalità individuate nell'informativa.

Elenco dei dati richiesti
Sezione 1
Dati identificativi socio (nominativo, data anagrafici, indirizzo cod. fiscale carta identità)
Dati strettamente necessari

Sezione 2
Dati facoltativi a tutela del cliente
cellulare , mail

Firma_____ □ **SI** □ **NO**

Consenso e modalità di acquisizione

La raccolta del consenso avviene al momento dell'iscrizione del Socio, tramite firma su apposito modello (vedi sopra), una copia originale viene conservata nel fascicolo del socio e una copia viene data all'interessato. Copia del modello è reperibile anche dal sito web.

Requisiti più stringenti per trasferire dati verso Paesi Terzi
Non ricorrono

Cookies

Cookie cassacoop 10/05/2018

Tweet

Cookie summary for:

Cassacoopatc.it

FIRST PARTY COOKIES

0

more info on first party cookies

THIRD PARTY COOKIES

0

more info on third party cookies

THIRD PARTY REQUESTS

0

more info on third party requests

Cookie details

0 ***Local Cookies***

No cookies found.

0 **Third-party Cookies**

No cookies found.

0 **Third-party Requests**

Found no requests.

Cookie-checker.com collected this information on **05-10-2018**.

©2018 Inversive Media - All rights reserved. Like this product? Please share!

Web Cookies Scanner

All-in-one free web application security tool. Web application vulnerability and privacy scanner with support for HTTP cookies, Flash, HTML5 localStorage, sessionStorage, CANVAS, Supercookies, Evercookies. Includes a free SSL/TLS, HTML and HTTP vulnerability scanner and URL malware scanner.

- ·0 Home
- ·1 API
- ·2 Cookies
- ·3 Web intelligence
- ·4 Threat intelligence
- ·5 GDPR
- ·6 Do-Not-Track (DNT)
- ·7 Docs
- ·8 Contact

Cookie and Security Scan Report

http://www.cassacoopatc.it/

·9 Privacy

·10 Security

Privacy Impact Score

A

Privacy Impact Score is a score reflecting overall cookie-related impact of the website relative to other websites, primarily taking into account the number of third-party domains it reports to and number of persistent cookies it sets. See Privacy Impact Score article for more details.

Third-party domains

0

Persistent cookies

0

Session cookies

0

Third-party domains is the count of organisations allowed by the webmaster to trace your across the site. These cookies may be set for various purposes, like tracking ads displayed on the website, collection of statistics, targeted advertising etc. This website allows 0 other websites to track your activity.

Persistent cookies are the cookies that are preserved through browser shutdowns. This means, even if you close this page today and ever return there in future, the website will know you're a returning visitor. This may be used for "remember me" features, as well as persistent user tracking. These cookies, especially if set by third party organisations, are powerful tool for monitoring your activities across all the websites you visit. This website sets 0 persistent cookies with average life-time of 0 days and longest 0 days.

Session cookies are cleared when you close your browser and allow the website to identify user's state — such as logged-in users. They are mostly considered harmless because they cannot be used for long-term user tracking. This site sets 0 session cookies.

Last fetched: 2018-05-10T10:12:10.625804+00:00

Refresh

HTTP status: 200 200 OK

HTTP security-related headers assessment

Security score

0