
Università Politecnica delle Marche

Facoltà di Ingegneria

Corso di Laurea Triennale in Ingegneria Gestionale

# Adeguamento delle iscrizioni online alle norme GDPR

# Adaptation of online applications to GDPR norms

Relatore:
Prof. Primo Zingaretti

Laureanda:
Emanuela Mariotti

Anno Accademico 2018/2019

*A mia madre e a mio padre, senza i quali non sarei qui oggi.*

*A mia sorella, a mia nonna e al mio fidanzato che, a modo loro, mi hanno sempre sostenuta nello studio, nel lavoro e nella vita.*

Un ringraziamento particolare va al Professor Zingaretti per la supervisione del progetto e per l'attenzione dedicata ad ogni minimo dettaglio, in circa nove mesi di lavoro.

# ABSTRACT

In questa tesi si descrive l'implementazione di una sezione del sito del Circolo Universitario di Ancona (CRUA - https://www.crua.univpm.it/) che permette l'iscrizione di nuovi utenti al Circolo stesso e il suo adeguamento alle norme del Regolamento Generale sulla Protezione dei Dati (o General Data Protection Regulation – GDPR), come esempio di applicazione di un procedimento più ampio che interessa tutto il World Wide Web.

Il 24 maggio 2016, infatti, è entrato in vigore il Regolamento Generale sulla Protezione dei Dati (richiamato spesso in questa tesi come "Regolamento", "Regolamento UE 679/2016" o "GDPR") che modifica profondamente il "Codice in materia di protezione di dati personali" del D. Lgs. 196/2003.

A seguito dell'applicazione delle norme da parte di tutti gli Stati membri dell'Unione Europea entro il 25 maggio 2018, si è reso necessario adeguare anche le iscrizioni effettuate online dagli utenti di associazioni, aziende e servizi. Di conseguenza, nel caso del CRUA, al fine di informatizzare un processo di iscrizione che ormai da troppo tempo si attuava con "carta e penna", si è deciso di integrarlo nel preesistente sito del Circolo, implementando un'interfaccia utente del tipo *web-form* secondo le norme GDPR, accessibile dagli utenti che vogliono iscriversi nel *front-end* (parte visibile da chiunque e raggiungibile all'indirizzo *web* del sito) e ai titolari e responsabili del trattamento dati nel *back-end* (parte di amministrazione di un sito accessibile solo da amministratori del sito web).

Il successivo D. Lgs. n.101 del 10 agosto 2018, tra le nuove modifiche che introduce al Regolamento UE 679/2016, qualifica i dati personali come "diritti fondamentali dell'uomo" e responsabilizza il soggetto che *tratta* i dati tramite l'applicazione di principi introdotti dal GDPR.

Il trattamento dei dati personali è il concetto chiave ed è soggetto all'applicazione, da parte del titolare e del responsabile, di misure tecniche e organizzative atte a garantire un livello di sicurezza proporzionato al rischio.

Comunque, il Regolamento non fornisce dei veri e propri criteri di adeguamento, bensì innova i principi applicabili al trattamento dei dati personali indicati dal decreto legislativo e in parte ne introduce di nuovi, riconoscendo agli interessati il diritto di accesso, di limitazione del trattamento, di cancellazione e di portabilità.

Per comprendere le norme provenienti da un testo di natura giuridica (corrispondente a quella del Regolamento) occorre capacità interpretativa in ambito giurisprudenziale ma, allo stesso modo, capacità tecnica in ambito informatico e gestionale per la loro applicazione.

La sfida che si affronta in questa tesi, tramite la tecnologia informatica, è infatti quella dell'applicazione di norme giuridiche molto vaghe e generiche per quanto concerne i riferimenti pratici.

Nella messa in opera del *General Data Protection Regulation* è necessario garantire il perseguimento degli obiettivi per i quali esso è stato concepito; sebbene vi siano molte definizioni e caratteristiche dei ruoli, dei diritti e dei doveri che accompagnano l'introduzione di nuove figure che intervengono in questo campo, non è ben chiaro come esse debbano comportarsi nei vari casi che possono incontrare nella realtà.

Questo accade a causa dell'introduzione del principio dell'*accountability* (traducibile come "principio di responsabilizzazione" e si approfondisce nel primo capitolo di questo testo) che è alla base del Regolamento: per la soddisfazione di tale principio è infatti incompatibile l'adozione di modelli standard e "preconfezionati", poiché la responsabilizzazione degli individui che gestiscono, o meglio "trattano", i dati deve avvenire proprio tramite un'applicazione delle norme che deve essere ideata e strutturata a misura dello specifico caso considerato.

Tuttavia, è importante precisare che per raggiungere l'obiettivo non si deve partire dal precetto normativo (come potrebbe sembrare), bensì dallo scopo ultimo del Regolamento: la tutela del dato. Successivamente, procedendo a ritroso, si individuano le misure da adottare, in conformità alle disposizioni del Regolamento.

In proposito, occorre specificare che l'ambito di applicazione del GDPR non è esclusivamente quello digitale, sebbene nel presente testo sia l'unico che si approfondisce: nell'art. 2 del GDPR viene precisato che "il presente Regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento automatizzato di dati personali contenuti in un archivio o destinati a figurarvi" e che, in particolare, è applicabile solo ai dati personali dei soggetti che si trovano nell'Unione Europea.

Illustrate le molte figure che il Regolamento introduce e definisce, di cui la più importante è quella dell'"interessato" (poiché sono i dati personali di quest'ultimo a venire tutelati dalle norme in questione), nel secondo paragrafo si analizza l'unico e reale diritto/dovere dell'utente: essere informato dei dati personali che potrebbe comunicare (e a chi potrebbe comunicarli) semplicemente visitando una specifica pagina o piattaforma web (o portando a termine un'iscrizione tramite essa) e accettarne consapevolmente il trattamento.

Nel terzo paragrafo si discute brevemente a proposito della cosiddetta "analisi del rischio", un procedimento complesso che i gestori di siti *web* hanno l'obbligo di applicare per capire a quali rischi espongono i loro utenti tramite la struttura stessa dell'ambiente che mettono a disposizione.

Si approfondisce dunque la tematica centrale della tesi nel secondo capitolo, descrivendo come si è arrivati allo stato attuale di implementazione di una piattaforma di iscrizione in un sito *web* realmente esistente, essendosi posti nella situazione di doverlo gestire e adeguare alle sopracitate norme. Qui si affronta anche la risoluzione delle

problematiche legate all'adeguamento alle norme GDPR vero e proprio, come ad esempio quella relativa all'iscrizione di un minore: dopo aver effettuato il calcolo dell'età, il sistema invia e-mail e messaggi specifici per far sì che sia il genitore a formalizzare l'iscrizione.

I risultati ottenuti sono visibili nel terzo capitolo.

In conclusione, il sito è stato implementato in modo da risultare conforme sia alle norme GDPR che alle disposizioni del CRUA. Sarebbe possibile accrescere il potenziale del sito web in molti modi in futuro, come ad esempio tramite l'introduzione di un metodo di pagamento online; ogni implementazione, però, richiede che a monte sia compiuta un'analisi del rischio, per cercare di applicare al meglio tutte le norme del Regolamento e di proteggere i dati personali con i mezzi a disposizione.

In appendice si riportano i riferimenti tecnico-informatici che costituiscono il progetto, corredati dalle sezioni più significative del codice scritto in linguaggio *php*, *html* e *css*.

# INDICE

# INTRODUZIONE

L'adeguamento alle norme del Regolamento Generale sulla Protezione dei Dati (RGPD o, dall'inglese, GDPR che sta per *General Data Protection Regulation*) è un argomento attuale di cui tutti coloro che sono entrati in contatto con il *World Wide Web* in territorio europeo, dal 2016 ad oggi, hanno visto gli effetti.

I piccoli messaggi in sovrimpressione situati nella parte alta (o bassa) di ogni pagina *web* che visitano, che generalmente riportano una richiesta di accettazione dei cosiddetti *cookie* (componenti identificative utilizzate dalle applicazioni *web* per archiviare e recuperare informazioni a lungo termine relative a chi interagisce con esse), sono il frutto più immediato ed evidente dell'applicazione delle norme del GDPR.

La conoscenza del Regolamento che si è obbligati a detenere, nell'ambito del *web*, cambia in modo notevole a seconda del caso in cui ci si trova: si è un semplice utente che naviga in *Internet* o si è il gestore di qualche sito o piattaforma *web*?

Qualora non si avesse l'onere di gestire un sito *web*, la questione sarebbe la più semplice, poiché l'utente sarebbe tenuto soltanto a conoscere i suoi diritti (che il GDPR si occupa di definire e far rispettare, grazie alle autorità di controllo da esso stesso preposte) per poter scegliere se farli valere o meno. Ciò che la maggior parte degli utenti vede dunque, navigando in un qualsiasi sito *web* è solo la "punta dell'iceberg" di una serie di norme articolate e complesse che costituiscono il Regolamento.

Nel caso di gestori di siti o piattaforme web, si presenterebbe quindi l'obbligo di applicare queste norme, per far sì che i dati personali degli utenti che navigano nel loro sito siano protetti e non soggetti a divulgazioni non autorizzate.

È anche vero però che, sebbene la figura con meno obblighi sia quella dell'utente, essa è, al tempo stesso, la protagonista del GDPR.

Si affronta un *excursus* sul Regolamento Generale per la Protezione dei Dati nel primo capitolo, approfondendo gli argomenti fondamentali nei sottoparagrafi, dopodiché si ragiona sulle modalità di realizzazione e sulle motivazioni del progetto della piattaforma di iscrizione al CRUA per renderla conforme alle specifiche richieste e contemporaneamente al GDPR; se ne vedono poi i risultati nel terzo capitolo.
Si arriva alla conclusione del lavoro nell'ultimo capitolo, dopo un'attenta analisi del testo del Regolamento e dei suoi aggiornamenti.

# 1. GENERAL DATA PROTECTION REGULATION (GDPR)

Il GDPR è una normativa che nasce con l'intento di garantire e tutelare i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
A norma dell'art.4 del Regolamento (UE) 2016/679 del Parlamento Europeo, per dato personale s'intende:

> Qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale e sociale".

Come invece accadeva nel D. Lgs 196/2003, nel GDPR non vengono menzionati i "dati sensibili" perché la denominazione è stata sostituita con quella di "dati particolari" e, nell'articolo 9 del Regolamento UE 679/2016, si specifica che:

> È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
> Il divieto non si applica in presenza di consenso esplicito o di necessità per assolvere gli obblighi.

Nel caso venissero trattati dati particolari, anche in presenza di consenso, è necessario adottare misure di sicurezza aggiuntive per la loro protezione, rispetto ai dati non particolari.

Di seguito viene riportato uno schema della classificazione dei dati personali. [8, 11, 17, 21]

| Identità | Categoria di dato personale |
|---|---|
| | **Dati comuni** |
| Pubblica | Dati pubblici |
| | Dati identificativi generici |
| Culturale/lavorativa | Formazione ed esperienze di lavoro |
| | Attività lavorativa |
| Economica | Identificativi finanziari |
| Online | Identificativi online |
| Formale | Documenti di identità |
| | **Dati particolari** |
| Etnica | Origine razziale o etnica |
| Politica | Opinioni politiche |
| | Appartenenza sindacale |
| Sessuale | Orientamento sessuale |
| | Vita sessuale |
| Religiosa o Filosofica | Convinzioni religiose |
| | Convinzioni filosofiche |
| Biometrica | Dati fisici |
| | Dati biometrici |
| Giudiziaria | Dati giudiziari |
| Sanitaria | Dati sanitari |
| | Dati genetici |

I principi applicabili al trattamento dei dati personali, che devono permearlo dalla fase iniziale a quella finale, sono indicati dall'art. 5 del Regolamento.

> I dati personali devono essere:
> a) trattati in modo lecito, equo e trasparente nei confronti dell'interessato ("liceità, equità e trasparenza");
> b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità; un ulteriore trattamento dei dati personali per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche non è, conformemente all'articolo 83, paragrafo 1, considerato incompatibile con le finalità iniziali ("limitazione della finalità");
> c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
> d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");
> e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche, conformemente all'articolo 83, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal regolamento a tutela dei diritti e delle libertà dell'interessato ("limitazione della conservazione");

Essi sono dunque, rispettivamente:

a. il principio di liceità, i cui presupposti di legittimità possono essere riassunti nella tabella seguente, tratta dalla pagina n. 31 del libro di De Stefani F., *Le regole della privacy – Guida pratica al nuovo GDPR* Milano: Editore Ulrico Hoepli, 2018 [6];

| | |
|---|---|
| Consenso | Si crea un vincolo contrattuale |
| Esecuzione di un contratto o misure precontrattuali | Non è necessario il consenso |
| Adempimento di un obbligo legale del titolare | |

| | |
|---|---|
| Salvaguardia di interessi vitali | |
| Esecuzione di un interesse pubblico o connesso a pubblici poteri | |
| Perseguimento del legittimo interesse | |

b. il principio di finalità: le caratteristiche della finalità possono essere riassunte nella tabella seguente, tratta dalla pagina n. 34 del libro di De Stefani F., *Le regole della privacy – Guida pratica al nuovo GDPR* Milano: Editore Ulrico Hoepli, 2018 [6];

| | |
|---|---|
| Deve essere esplicita | |
| Deve essere comunicata:<br>• all'interessato;<br>• prima dell'inizio del trattamento | |
| Può cambiare e la nuova finalità **non è compatibile** con quella iniziale | È necessario un nuovo consenso |
| Può cambiare e la nuova finalità **è compatibile** con quella iniziale | Non è necessario un nuovo consenso |

c. il principio di minimizzazione;
d. il principio di esattezza;
e. il principio di conservazione.

Un ulteriore importante principio introdotto dal Regolamento (art. 25, par. 1 GDPR), da applicare fin dall'inizio del trattamento dei dati per garantirne la riservatezza e l'integrità, è quello relativo alla cosiddetta *Privacy by Design* (Protezione dei dati fin dalla progettazione), ovvero l'obbligo di individuare e applicare le misure tecniche e organizzative più idonee ad attuare in modo efficace i principi della protezione dei dati, di

integrare nel trattamento le garanzie necessarie a soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati. Inoltre, la progettazione deve garantire un livello di sicurezza adeguato al rischio di violazione dei dati trattati, passando attraverso l'"Analisi del rischio" (descritta più avanti). La *Privacy by Design* pone così la persona fisica, proprietaria dei dati, al centro del sistema di tutela, ed obbliga il titolare a un impegno effettivo e non solo formale.

La *Privacy by Default* (art. 25, par. 1 GDPR) è invece il principio che prevede, "per impostazione predefinita", che il titolare tratti i dati personali solo nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. La progettazione del sistema di trattamento dei dati deve quindi garantire la non eccessività dei dati raccolti, in modo che l'interessato riceva un alto livello di protezione anche se egli non si adopera attivamente per limitare la raccolta dei dati.

Anche se si acquisisse la certificazione (ex art. 42 del "Codice in materia di protezione dei dati personali), essa potrebbe venire utilizzata come elemento per dimostrare la conformità ai requisiti *by design* e *by default*, ma "non ridurrebbe la responsabilità del titolare e del responsabile del trattamento dati e lascerebbe impregiudicati i compiti e i doveri delle autorità di controllo" (art. 42, par. 4 GDPR). [22, 24]

Di seguito vengono individuate le figure principali definite dal Regolamento.

- *Interessato* è la persona fisica a cui si riferiscono i dati personali;
- *Titolare al trattamento dati* è la persona o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- *Responsabile del trattamento dati* è la persona o altro organismo cui il titolare affida, anche all'esterno della sua struttura organizzativa, per la particolare esperienza o capacità, compiti di gestione e controllo del trattamento dei dati;

- *Incaricato* è il dipendente o il collaboratore - che, per conto del titolare, elabora o utilizza materialmente i dati personali sulla base delle istruzioni ricevute dal titolare e/o dal responsabile;
- *Destinatario* è la persona o altro organismo che riceve comunicazione di dati personali. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- *Responsabile della Protezione dei dati* (DPO – *Data Protection Officer*) è la persona fisica esperta e indipendente che fornisce consulenza al titolare e al responsabile sulle corrette modalità di trattamento dei dati e garantisce il rispetto degli obblighi derivanti dal Regolamento (non è tuttavia responsabile né destinatario di sanzioni per il mancato adeguamento/rispetto del GDPR da parte del titolare o del responsabile). È una figura obbligatoria soltanto nei casi in cui il trattamento dei dati è effettuato da un ente pubblico (escluse le autorità giurisdizionali), se l'attività principale del titolare consiste in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala e se l'attività principale del titolare consiste nel trattamento su larga scala di dati sensibili o giudiziari;
- *Designato* è un soggetto (specificatamente incaricato per iscritto e istruito sugli obblighi da rispettare dal titolare o dal responsabile) che ha accesso ai dati personali trattati dal titolare o dal responsabile del trattamento e che effettua operazioni di trattamento sotto la loro autorità;
- *Rappresentante* è la persona stabilita nell'Unione che, designata dal titolare o dal responsabile del trattamento per iscritto ai sensi

dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del regolamento 679/16. È una figura obbligatoria soltanto nei casi in cui titolare e responsabile hanno sede fuori dall'UE, se vengono offerti beni o servizi a residenti nell'UE o se vengono effettuati monitoraggi di abitudini relative a soggetti residenti nell'UE;

- *Terzo* è la persona o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- Le *Autorità di Controllo* sono organismi indipendenti, costituiti in ciascuno Stato membro, incaricati di sorvegliare l'applicazione del GDPR. In Italia l'Autorità di Controllo è il Garante della Privacy (www.garanteprivacy.it);
- L'*Organismo di Controllo* è un soggetto accreditato presso l'Autorità di Controllo o presso Accredia che ha il compito di monitorare la conformità delle attività di trattamento al codice di condotta al quale il titolare ha aderito;
- Il *Comitato Europeo per la Protezione dei Dati* è un organismo indipendente che sovrintende le attività di tutte le Autorità di Controllo dei singoli Stati membri.

I diritti su cui si fonda il GDPR, che coinvolgono queste figure sono [7, 12]:

- Diritto alla trasparenza (artt. 5, 12 Regolamento UE 679/2016) per conoscere (quindi sapere chi avrà effettivamente accesso ai suoi dati) e comprendere le finalità per le quali vengono trattati i dati, monitorarli e decidere cosa farne.
- Diritto all'informazione (artt. 12, 13, 14 Regolamento UE 679/2016) per l'Interessato che può richiedere al titolare e al responsabile tutte le informazioni relative ai dati che sono stati raccolti. Inoltre, può richiedere informazioni che non gli sono state fornite a causa della mancanza di esaustività a monte;

- Diritto di accesso (art. 15 Regolamento UE 679/2016) ai dati da parte dell'Interessato per fornirgli strumenti di controllo sui suoi dati. In particolare, si tratta del diritto di accesso alle finalità del trattamento, alle categorie di dati trattate, ai destinatari dei dati, al periodo di conservazione, alla possibilità di proporre reclamo;
- Diritto di rettifica (art. 16 Regolamento UE 679/2016) che riconosce all' Interessato, il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano (senza ingiustificato ritardo) oppure l'integrazione dei dati, ovvero l'aggiornamento dei dati non più attuali. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa;
- Diritto all'oblio (art. 17 Regolamento UE 679/2016) per l'Interessato che può ottenere dal titolare la cancellazione dei dati personali che lo riguardano (in originale "*right to be forgotten*") da parte del titolare che ha il dovere di eliminarli. Questo diritto si applica se i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati, se sono stati trattati illecitamente, se si deve adempiere un obbligo legale, se l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento, se l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2 (*marketing* diretto);
- Diritto di limitazione al trattamento (art. 18 Regolamento UE 679/2016) richiedibile al titolare del trattamento dall'Interessato quando quest'ultimo contesti l'esattezza dei dati personali (per il

periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali) o quando il trattamento è illecito e l'Interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo, oppure quando l'Interessato, oppostosi al trattamento ai sensi dell'articolo 21, paragrafo 1, è in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'Interessato;

- Diritto alla portabilità dei dati (art. 20 Regolamento UE 679/2016) per l'Interessato che può ricevere i dati personali che lo riguardano forniti da un titolare del trattamento e può trasmetterli a un altro titolare del trattamento se è un trattamento effettuato con mezzi automatizzati e se si basa su un consenso o su un contratto;
- Diritto di opposizione (art. 21 Regolamento UE 679/2016) dell'Interessato se necessario per l'esecuzione di un compito di interesse pubblico, se connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento o se necessario per il perseguimento del legittimo interesse del titolare o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiede la protezione dei dati personali (in particolare se minore), eccetto il caso in cui il trattamento è effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Ponendosi nell'ottica del caso CRUA e prendendo a modello i quesiti posti nelle pagine n. 88, 89, 90, 91, 92 e 93 del libro Gradozzi F., Leonarduzzi S., Libertini G., *Privacy in regola,* Polonia: Amazon Fullfillment, 2019 [16], si fornisce una risposta a ciascuno di essi e si prova così ad effettuare una sorta di verifica sull'applicazione degli adempimenti dettati dalle norme del GDPR.

## 1.1. GESTIONE DEI DATI

*"SEI UN PROFESSIONISTA, UN IMPRENDITORE, UN ENTE PUBBLICO O UN'ASSOCIAZIONE E GESTISCI INFORMAZIONI DI QUALSIASI TIPO RIGUARDANTI PERSONE FISICHE VIVENTI DOMICILIATE IN UNO DEI VENTOTTO STATI MEMBRI DELL'UNIONE EUROPEA?"*

*SÌ*: è necessario adeguarsi alle nuove norme.

Definire il GDPR "legge *privacy*" è quantomeno riduttivo. Infatti, come già detto, esso esplica i requisiti per la messa in opera di un vero e proprio sistema di gestione della protezione dei dati in senso ampio e completo. Le modalità con cui avviene l'adeguamento sono dunque rimesse al soggetto che deve effettuare il trattamento e le deve individuare in base alle caratteristiche della propria organizzazione. Questo "principio di responsabilizzazione" [19] sta alla base di tutto il Regolamento ed è chiamato "Principio di *accountability*". La valutazione finale sulle procedure da mettere in atto per adeguarsi al nuovo regolamento è perciò totalmente a carico del titolare e del responsabile del trattamento dei dati. Essi sono tanto liberi quanto responsabili delle scelte che compiono: devono documentare le loro azioni e dimostrarne la rispondenza ai requisiti richiesti dalla normativa.

### ❖ 1.1.1. RAPPRESENTANTE:

*"LA SEDE DELLA TUA ORGANIZZAZIONE È SITUATA AL DI FUORI DELL'UNIONE EUROPEA E OFFRE BENI O SERVIZI A PERSONE DOMICILIATE NELL'UNIONE EUROPEA O EFFETTUA MONITORAGGI DI ABITUDINI RELATIVE A SOGGETTI RESIDENTI NELL'UNIONE EUROPEA?"*

*NO*: non è necessario nominare un Rappresentante (una persona fisica o giuridica stabilita nell'UE che rappresenti l'associazione in relazione agli obblighi derivanti dalla normativa).

### ❖ 1.1.2. TITOLARE O CONTITOLARE:

*"DEFINISCI DA SOLO I FINI E I MEZZI DEI TRATTAMENTI DI DATI PERSONALI O LO FAI INSIEME AD UN ALTRO IMPRENDITORE O PROFESSIONISTA?"*

*SÌ*: se la gestione non è condivisa, non è necessario stipulare un accordo con i partner per stabilire le rispettive responsabilità e compiti.

### ❖ 1.1.3. RESPONSABILE DEL TRATTAMENTO:

*"PER IL TRATTAMENTO DEI DATI PERSONALI HAI DELEGATO UN ALTRO SOGGETTO?"*

*SÌ*: è necessario nominare per iscritto (attraverso un contratto) un responsabile del trattamento.

### ❖ 1.1.4. DATA PROTECTION OFFICER:

*"SEI UN ENTE PUBBLICO? O LA TUA ATTIVITÀ PRINCIPALE CONSISTE IN TRATTAMENTI CHE RICHIEDONO IL MONITORAGGIO REGOLARE E SISTEMATICO SU LARGA SCALA DI SOGGETTI PRIVATI? O LA TUA ATTIVITÀ PRINCIPALE CONSISTE NEL TRATTAMENTO, SU LARGA SCALA, DI DATI SENSIBILI O GIUDIZIARI?"*

*NO*: non è necessario nominare un *Data Protection Officer*.

### ❖ 1.1.5. COLLABORATORI:

*"HAI DEI COLLABORATORI (ES. DIPENDENTI, TIROCINANTI) CHE LAVORANO SUI DATI PERSONALI CHE GESTISCI?"*

*NO*: non è necessario nominarli come designati.

## 1.2. INFORMATIVA E CONSENSO

*"UTILIZZI UNA CORRETTA INFORMATIVA SCRITTA CHE SOTTOPONI ALLE PERSONE DI CUI TRATTI I DATI PERSONALI? UTILIZZI UN APPOSITO MODULO PER RACCOGLIERE IL CONSENSO QUANDO NECESSARIO?"*

*SÌ*: non ci sono altri obblighi al riguardo.

Per quanto riguarda i siti web, tutti devono avere una propria *privacy policy* che spieghi la tipologia di dati raccolti, il motivo della raccolta, il modo in cui vengono trattati e ottenuti tali dati, come e per quanto tempo saranno conservati, se saranno ceduti a soggetti terzi e a quali condizioni. Il caso di un sito web è particolare perché l'informativa data online potrebbe non essere la sola da fornire all'utente. Essa è necessaria ogni qualvolta l'utente "lasci" qualche dato personale, sia in maniera volontaria che involontaria ("automatica").

<table>
<tr><td rowspan="4">Utente che naviga in un sito web</td><td rowspan="2">Non lascia dati</td><td>Volontari</td><td rowspan="2">Nessuna informativa</td></tr>
<tr><td>Involontari</td></tr>
<tr><td rowspan="2"><u>Lascia dati</u></td><td>Volontari</td><td rowspan="2">È necessaria un'informativa con indicazione specifica delle finalità del trattamento</td></tr>
<tr><td>Involontari</td></tr>
</table>

Non è previsto alcun obbligo di forma per la redazione dell'informativa se non quello relativo alla concisione e alla chiarezza. Di seguito viene riportato l'elenco, tratto dalla tabella di pagina n. 61 del libro di De Stefani F., *Le regole della privacy: Guida pratica al nuovo GDPR*, Hoepli: Milano, 2018 [6], degli elementi che devono essere contenuti nell'informativa sulla *privacy* per un sito *web*.

- Estremi identificativi del titolare al trattamento e del responsabile al trattamento;
- Eventuale esistenza di un DPO
- Finalità del trattamento;
- Modalità del trattamento (in caso di più finalità, riassumere finalità e modalità del trattamento);
- Base giuridica del trattamento;

- Possibilità di trasferimento a Paesi terzi;
- Possibili conseguenze del trattamento sull'Interessato;
- Nel caso di profilazione, indicazione delle logiche che sono alla base del trattamento;
- Diritti dell'Interessato.

Secondo l'art. 42 del GDPR:

> Per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. In particolare, nel contesto di una dichiarazione scritta relativa a un'altra questione dovrebbero esistere garanzie che assicurino che l'interessato sia consapevole del fatto
> di esprimere un consenso e della misura in cui ciò avviene. In conformità della direttiva 93/13/CEE del Consiglio (1) è opportuno prevedere una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive. […]

La raccolta del consenso via internet può essere effettuata tramite due procedure, quella di *opt-in* e quella di *opt-out* [6].
L'*opt-in* è il processo che descrive l'azione di un utente che presta il suo consenso in maniera volontaria. Le caselle "*check-box*" non preselezionate sono un esempio comune di come il meccanismo di *opt-in* viene implementato. Una volta apposta la spunta alla casella, l'azione viene considerata come consenso alla richiesta esplicitata dalla check-box stessa. Questa procedura può essere usata per ricevere il consenso dagli utenti in diverse occasioni, come ad esempio il consenso per i *cookies*, per l'accettazione delle informative legali o della *privacy*, per la sottoscrizione alla *newsletter* di un sito, ecc. ed è sufficiente a rendere regolare l'accettazione delle condizioni, stando a quanto riportato nel Considerando 25, pagina 14 del GDPR.

> Il consenso dovrebbe essere espresso mediante un'azione positiva inequivocabile con la quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare che i dati personali che lo riguardano siano oggetto di

> trattamento, ad esempio mediante dichiarazione scritta, anche elettronica, 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 questo contesto che l'interessato accetta il trattamento proposto. […]
> Se il consenso dell'interessato è richiesto con modalità elettronica, la richiesta deve essere chiara, concisa e non disturbare inutilmente il servizio per il quale il consenso è espresso.

L'*opt-out*, invece, è il processo tramite cui un utente rinuncia o rifiuta di fornire il consenso per determinate azioni. Questa procedura permette all'utente di avere un grande controllo sui propri dati e sulle altre opzioni relative alla *privacy*. Solitamente, nei siti web, si mette in pratica in due modi: mettendo a disposizione dell'utente caselle preselezionate da poter deselezionare oppure permettendo all'utente di ritirare il consenso precedentemente fornito.

Dall'entrata in vigore del GDPR, in rete si possono trovare diversi servizi (gratuiti e a pagamento) che offrono un aiuto concreto per l'adeguamento alle norme. Un servizio online a pagamento molto famoso per questo adempimento è "*Iubenda*" (https://www.iubenda.com/it/), ma delle alternative efficaci e gratuite per ciò che riguarda la *privacy policy* e i *cookie policy* dei siti internet sono "*Nibirumail*" (https://nibirumail.com/cookies/ - permette di individuare gratuitamente i cookie di un sito web, nella sua versione gratuita offre *cookies* tecnici, *cookies policy* e *cookie banner* e, genera automaticamente e in base ai cookie rilevati, la pagina della *privacy policy*) e "*PrivacyPolicies*" (https://www.privacypolicies.com/ - permette di generare la *privacy policy* di un sito web, di un'*app* o di un *e-commerce*, inserendo alcune informazioni utili sul funzionamento di alcuni aspetti della gestione dei dati degli utenti).

### ❖ 1.2.1. TRASFERIMENTO DEI DATI ALL'ESTERO:

*"HAI NECESSITÀ DI TRASFERIRE I DATI CHE TRATTI AL DI FUORI DELL'UNIONE EUROPEA? AD ESEMPIO, TI AVVALI DI SERVIZI DI CLOUD COMPUTING, SITUATI FUORI DAI CONFINI DELL'UNIONE EUROPEA?"*

*NO*: non ci sono obblighi al riguardo. Altrimenti, si dovrebbe verificare che la Commissione Europea non abbia emesso una valutazione di adeguatezza degli standard di protezione del Paese estero verso cui si vogliano trasferire i dati e in caso ciò non fosse avvenuto, si dovrebbero fornire delle garanzie adeguate o acquisire il consenso specifico da parte dell'Interessato.

### ❖ 1.2.2. MINORI:

*"TRATTI DATI PERSONALI RIFERITI A SOGGETTI MINORI?"*

*SÌ*: è necessario implementare un sistema che consenta di verificare l'età dell'interessato e raccogliere il consenso al trattamento da parte dei genitori o di chi ne ha la potestà.

Secondo quanto indicato nell'art. 8 (Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione):

> Qualora si applichi l'articolo 6, paragrafo 1, lettera a) – CONSENSO – per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.
> Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore a 13 anni.
> Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.
> Non sono pregiudicate le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.

Il consenso al trattamento dei dati è valido se chi lo fornisce ha dai 14 anni in su (art. 2 quinquies del D.lgs. 10.08.2018 n. 101 - Consenso del minore in relazione ai servizi della società dell'informazione).
Se chi si iscrive avesse un'età inferiore ai 14 anni, dovrebbe inviare anche il modulo del consenso compilato e firmato dal genitore (o dalla persona che ha la potestà del minore).

> In attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale.

## 1.3. Analisi del Rischio

*"HAI SVOLTO UN'ACCURATA ANALISI SU COME GESTISCI I DATI PERSONALI E, IN PARTICOLARE, SU QUALI TIPOLOGIE DI DATI PERSONALI TRATTI (ES. DATI COMUNI, SENSIBILI, GIUDIZIARI), SULLA FONTE DALLA QUALE LI ACQUISISCI, SE LI GESTISCI IN FORZA DI UNA LEGGE O DI UN CONTRATTO, SUI POTENZIALI RISCHI CONNESSI ALLA TUA ATTIVITÀ DI TRATTAMENTO E SU QUALI MISURE DI PROTEZIONE HAI ADOTTATO?"*

*SÌ*: è possibile definire le misure tecniche e organizzative da adottare.

"Per "rischio" si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità per i diritti e le libertà" (art. 29 L.G. Gruppo di Lavoro). Nella sua individuazione bisogna considerare gli elementi che di fatto lo costituiscono, ovvero "origine, natura, gravità, probabilità, impatto sui diritti e sulle libertà degli interessati".

Secondo l'art. 32, comma 2 – Sicurezza sul trattamento:

> L'analisi del rischio serve a valutare l'adeguato livello di sicurezza, tenendo conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, dei dati personali trasmessi, conservati o comunque trattati.

Definito il *risk appetite*, ovvero quanto l'organizzazione è disposta ad esporsi all'impatto del realizzarsi di una minaccia, viene attribuito ad ogni minaccia il suo grado di probabilità potenziale di realizzarsi e quale è di conseguenza l'impatto che questo rischio avrebbe sull'organizzazione, in termini di riservatezza, integrità e disponibilità. Verificate quali misure sono state adottate per proteggere l'asset oggetto di valutazione, il rischio viene riclassificato, per verificare se l'impatto residuo è accettabile, secondo quanto definito dal risk appetite. Nel caso in cui l'impatto non sia accettabile, va pianificata una strategia tesa a mitigare il rischio, fino a renderlo accettabile. [19]

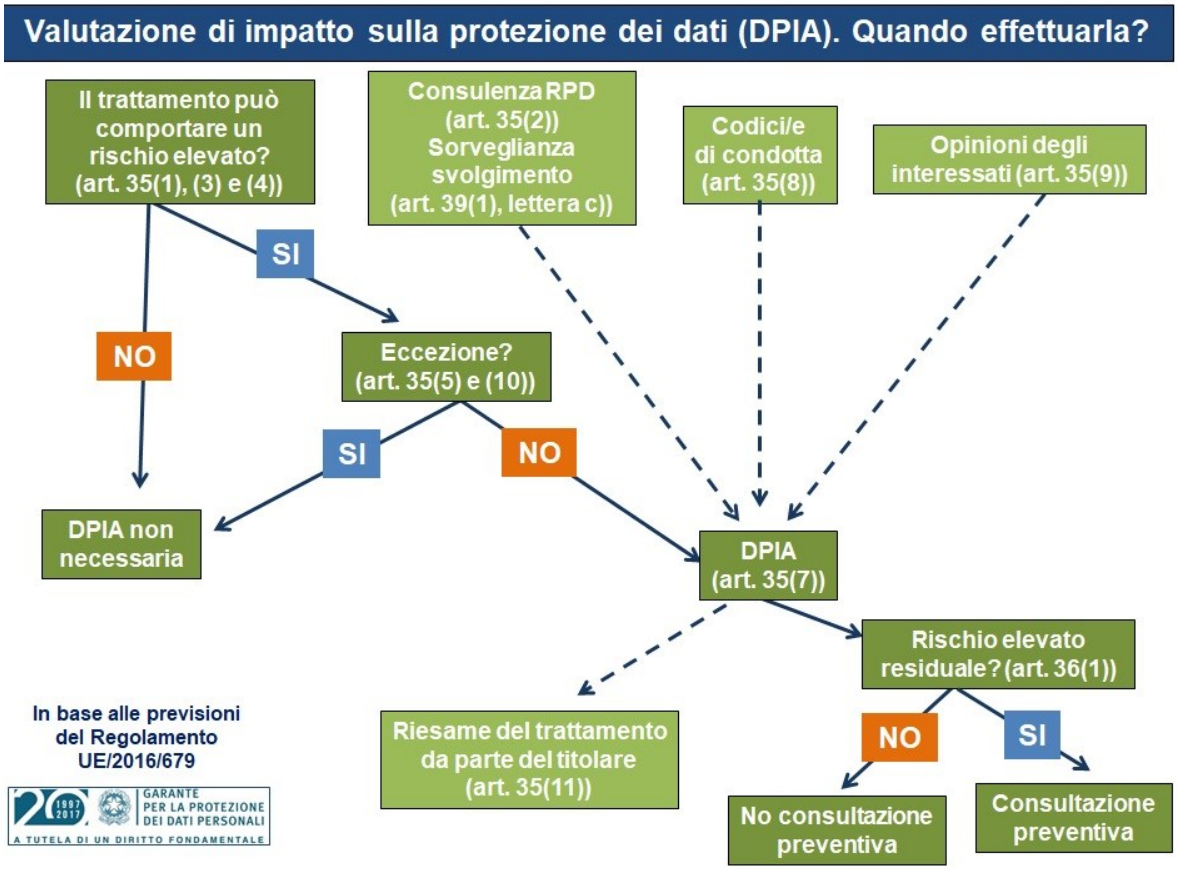
Se si dovesse riscontrare che il trattamento dei dati presenta un rischio elevato per i diritti e le libertà delle persone fisiche, si renderebbe necessario effettuare una valutazione d'impatto dei trattamenti previsti, sulla protezione dei dati personali ed eventualmente effettuare anche una consultazione preventiva.

La valutazione di impatto (DPIA – *Data Protection Impact Assessment*) è obbligatoria solo in alcuni casi (e l'obbligo vale anche per i trattamenti già in corso prima del 25 maggio 2018), individuabili dalla soddisfazione di almeno due tra i seguenti criteri:

1) Trattamenti di valutazione o di scoring (assegnazione di punteggi);
2) Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura;
3) Monitoraggio sistematico degli interessati;
4) Trattamento di dati sensibili o di natura estremamente personale;
5) Trattamenti di dati su larga scala;

6) Combinazione o raffronto di più trattamenti a partire da dati di origine diversa;
7) Dati relativi a soggetti (interessati) vulnerabili;
8) Uso di tecnologie innovative o applicazione di nuove soluzioni tecnologiche e organizzative;
9) Trattamenti che impediscono agli interessati di esercitare un diritto, di usufruire di un servizio o di attivare un contratto.

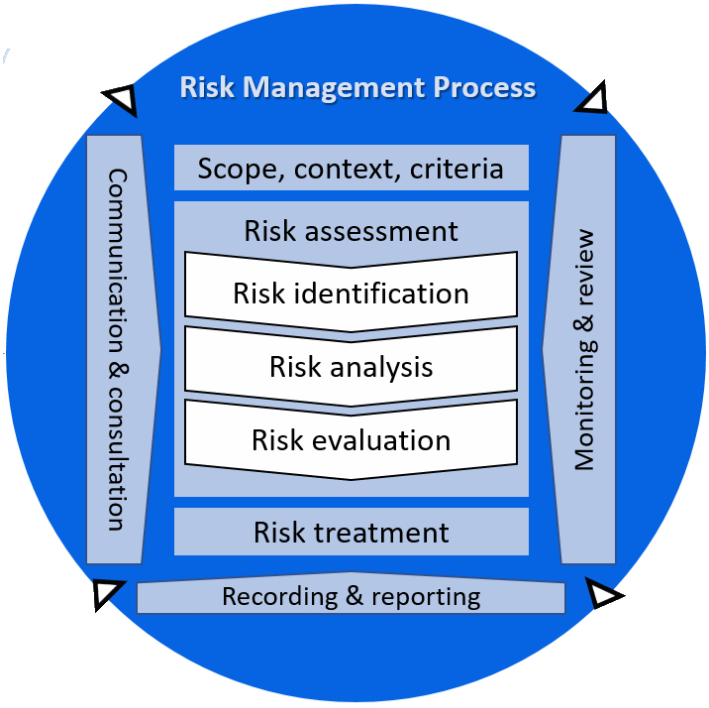
Purtroppo, nonostante l'esistenza di questi criteri, essi non sono esaustivi per determinare se un trattamento presenti effettivamente rischi elevati per gli Interessati e ciò comporta la necessità di effettuare un'analisi preliminare per decidere se fare la DPIA, anche se, in realtà, l'analisi è un obiettivo della stessa DPIA. [7, 17, 23, 24]




*Valutazione di impatto sulla protezione dei dati (DPIA). Quando effettuarla? - (https://www.garanteprivacy.it/regolamentoue/DPIA)*

Di seguito viene illustrato il modello *ISO 31000:2018* che aiuta le organizzazioni che ne fanno uso ad aumentare la probabilità di raggiungere gli obiettivi e di identificare le opportunità (effetti positivi) e le minacce (effetti negativi) per classificarle e usarle per analizzare il rischio. [8] Infatti, secondo il suddetto modello, il rischio viene visto in un'ulteriore ottica: viene definito come "effetto dell'incertezza sugli obiettivi". L'"effetto" è inteso come scostamento da quanto atteso sia in senso positivo che negativo. [17]

Il suddetto modello viene usato per avere delle linee guida nel campo delle analisi del rischio e per confrontare le misure adottate nella gestione del rischio con una base riconosciuta a livello internazionale, ma utilizzarlo non comporta il rilascio di alcuna certificazione.




*Schema dei processi per la gestione del rischio (Modello ISO 31000:2018) – Analisi del contesto (Scope, context, criteria), Valutazione del rischio (Risk assessment), Identificazione del rischio (Risk identification), Analisi del rischio (Risk analysis), Ponderazione del rischio (Risk evaluation), Trattamento del rischio (Risk treatment), Comunicazione e consultazione (Communication and consultation), Monitoraggio e riesame (Monitoring and review), Registrazione e reportistica (Recording and reporting)* [17]

| RISK ASSESSMENT MATRIX | | | | |
|---|---|---|---|---|
| SEVERITY / PROBABILITY | Catastrophic (1) | Critical (2) | Marginal (3) | Negligible (4) |
| Frequent (A) | High | High | Serious | Medium |
| Probable (B) | High | High | Serious | Medium |
| Occasional (C) | High | Serious | Medium | Low |
| Remote (D) | Serious | Medium | Medium | Low |
| Improbable (E) | Medium | Medium | Medium | Low |
| Eliminated (F) | Eliminated | | | |

*Tabella di valutazione del rischio (Risk Assessment) –*
*Stima delle probabilità di occorrenza delle minacce e loro livello di pericolosità*
*(https://blog.v-comply.com/risk-assessment-matrix/)*

### ❖ 1.3.1. DATA BREACH:

*"HAI MESSO A PUNTO LE PROCEDURE TECNICHE ED ORGANIZZATIVE PER RILEVARE, COMUNICARE E RISOLVERE POSSIBILI PERDITE DI DATI?"*

SÌ: non è necessario predisporre le migliori soluzioni tecniche ed organizzative per far fronte a possibili perdite di dati (*data breach*) e per la notifica delle stesse all'Autorità di Controllo e, nei casi previsti, agli interessati a cui si riferiscono i dati.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento ha l'obbligo di comunicare la violazione all'Interessato senza ingiustificato ritardo. Per "violazione dei dati" (*data breach*) si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4 n. 12 del GDPR).

Dallo schema seguente, tratto dalle linee guida dell'art. 29 del Gruppo di Lavoro, si evidenziano le tipologie di *data breach*.

| | |
|---|---|
| **Confidentiality breach** | Nel caso in cui ci sia una rivelazione non autorizzata o fortuita di dati personali o un accesso non autorizzato agli stessi |
| **Availability breach** | Nel caso ci sia una perdita o la distruzione dei dati personali |
| **Integrity breach** | Nel caso in cui ci sia un'alterazione o una modifica non autorizzata o accidentale di dati personali |

A seconda del tipo di violazione occorsa, se l'Autorità di Controllo ritiene che essa presenti un rischio, può ordinare al titolare di provvedere alla comunicazione all'Interessato nell'ipotesi in cui non abbia ancora provveduto o in seguito a una valutazione diversa da quella effettuata dal titolare.

| | | |
|---|---|---|
| **Comunicazione** | A chi | Autorità |
| | | Interessato |
| | Quando | 72 ore successive |
| | | Senza ritardo |
| | Non è richiesta | Dati non personali<br>Dati anonimizzati<br>Dati crittografati |
| | Obbligatoria | Rischi elevati per le libertà e i diritti dell'Interessato |
| **Contenuto** | Art. 33.3 | Informazioni minime da fornire |

### ❖ 1.3.1. REGISTRO ATTIVITÀ TRATTAMENTO:

*"HAI UN'ORGANIZZAZIONE CON PIÙ DI 250 DIPENDENTI? O EFFETTUI IN MODO NON OCCASIONALE TRATTAMENTI DI DATI PARTICOLARI O RELATIVI A CONDANNE PENALI O REATI? O EFFETTUI TRATTAMENTI CHE POSSANO PRESENTARE UN RISCHIO PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE?"*

*NO*: non ci sono obblighi relativi al tenere i registri delle attività di trattamento, benché il Garante della *Privacy* suggerisca di redigerli comunque.

Nella raccomandazione fatta dal Garante della *Privacy* nella guida all'applicazione del Regolamento UE 679/2016 in materia di protezione dei dati personali è specificato che:

> La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali.
> Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta.
> I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

Integrando il Registro delle attività del trattamento con le analisi del rischio precedentemente svolte, è possibile utilizzare per gli stessi asset, per le stesse minacce e per le stesse probabilità (ed aggiungere quindi gli impatti specifici) quelli nell'ottica dell'interessato. [20] È fondamentale però, che il registro sia aggiornato periodicamente, in relazione all'evoluzione dei singoli trattamenti e alle misure che vengono adottate. Infatti il registro consente, *ex ante*, di effettuare, monitorare e aggiornare tutte quelle attività che sono indispensabili per rispettare le norme del Regolamento ed*, ex post*, di dimostrare quanto è stato fatto senza dover essere costretti a ricostruire attività particolari. Naturalmente, tanto più saranno minuziose le attività inserite nel registro, tanto maggiore sarà la possibilità di provare subito la propria attività di protezione dei dati. [7]
La violazione delle disposizioni riguardanti gli obblighi del titolare e del responsabile, quali la tenuta del Registro della attività di trattamento, la valutazione d'impatto e la consultazione preventiva, la nomina del responsabile della protezione dei dati e la messa in sicurezza dei dati

personali, previsti dagli articoli da 25 a 39, è soggetta a sanzioni amministrative pecuniarie fino a 10 milioni di euro. [10]

### ❖ 1.3.3. MISURE TECNICHE E ORGANIZZATIVE:

*"HAI INDIVIDUATO LE MISURE TECNICHE E ORGANIZZATIVE PER EVITARE I RISCHI INDIVIDUATI NELL'ANALISI CHE HAI EFFETTUATO?"*

> *SÌ*: si è *compliant* (conformi) con il GDPR e non è necessario individuare le misure di sicurezza più adatte al contesto professionale.

I principi illustrati dall'art. 5 del Regolamento trovano concreta applicazione nella predisposizione da parte del titolare e del responsabile delle misure tecniche e organizzative di cui parla l'art. 24 dello stesso Regolamento. Le misure devono essere "personalizzate", cioè individuate e adeguate rispetto alla situazione concreta del titolare e non è quindi possibile utilizzare modelli standard per la loro messa in opera. Inoltre, le misure devono fornire una tutela "attuale" e non possono scaturire da un adempimento che non si evolve nel tempo.
Di seguito si evidenziano quelle più importanti:

1) la pseudonimizzazione (tecnica che consiste nel conservare i dati in una forma che impedisce l'identificazione dell'Interessato senza la combinazione con informazioni aggiuntive [7, 9]) e la cifratura dei dati personali;
2) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
3) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
4) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

5) Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Inoltre, per la liceità del trattamento, deve sussistere almeno una delle basi giuridiche di cui all'art.6 del GDPR (es. il consenso dell'interessato). [4]


*Individuazione e gestione del rischio, Tutorial, slide – Garante Privacy* [16]

### ❖ 1.3.4. ESERCIZIO DEI DIRITTI:

*"HAI MESSO A PUNTO LE PROCEDURE TECNICHE E ORGANIZZATIVE PER CONSENTIRE LA TEMPESTIVA SODDISFAZIONE DELLE RICHIESTE DI ESERCIZIO DEI DIRITTI PRESENTATE DALL'INTERESSATO?"*

*SÌ*: le disposizioni del Regolamento in materia sono rispettate.

Dagli artt. 11 e 12 GDPR si apprende che il termine per la risposta all'interessato è un mese, estendibile fino a tre mesi in casi di particolare complessità. Il titolare deve sempre dare un riscontro all'interessato entro un mese dalla richiesta, anche in caso di diniego. Spetta al titolare valutare la complessità del riscontro all'interessato e l'ammontare dell'eventuale contributo da chiedere a quest'ultimo, ma solo se si tratta di richieste manifestamente infondate o eccessive o ripetitive, o se prevedono il rilascio di più copie dei dati personali nell'ipotesi di diritto di accesso. La risposta all'interessato deve essere data per iscritto (la forma orale è ammessa solo se espressamente richiesta dall'interessato), concisa, trasparente, facilmente accessibile ed espressa con un linguaggio semplice e chiaro. [3]

# 2. ISCRIZIONI ONLINE AL C.R.U.A.

Nell'era moderna si rende indispensabile stare costantemente al passo con l'evoluzione tecnologica e la "digitalizzazione" è il processo che riduce significativamente, tra gli altri, l'utilizzo del supporto cartaceo, ormai obsoleto.

Non possono dunque mancare di esservi sottoposte la registrazione e la conservazione, con relativi documenti, delle iscrizioni di utenti a piattaforme già digitali, come quella del sito del Circolo Ricreativo Universitario di Ancona.

Lo studio di questo processo di trasformazione è proprio ciò che sta al centro della seguente trattazione.

## 2.1. RISOLUZIONE DELLE PROBLEMATICHE RISCONTRATE

Il *web-form* per le iscrizioni al sito del Circolo Ricreativo Universitario di Ancona è incluso, grazie all'uso dell'"*iframe*", nel sito preesistente del Circolo stesso, avente una sua politica su *cookies* e *privacy* che l'utente può accettare o rifiutare.

L'*iframe* è un elemento *HTML* utilizzato per mostrare il contenuto di una pagina *web*, o di una qualsivoglia risorsa, all'interno di un riquadro collocato, a sua volta, in un'altra pagina principale [26] e per funzionare ha richiesto, all'amministratore del sito CRUA, l'installazione sul sistema di una libreria apposita che ne permettesse il riconoscimento.

L'intervento dell'amministratore di sistema si è reso necessario perché il sito CRUA è stato sviluppato in *Drupal* (piattaforma *software*, scritta in linguaggio *php,* che permette la creazione e distribuzione di complessi siti web dinamici [25]) che, a causa della sua struttura modulare, richiede la singola installazione di ogni "nuovo elemento".

All'inizio del progetto, per dare vita al *web-form*, si era pensato di compilare semplicemente una pagina del sito, sfruttando le funzionalità del *Drupal*. Si è poi preferito procedere programmando in linguaggio *php* e facendo l'integrazione del contenuto creato tramite l'*iframe*, al fine di non essere condizionati dalle regole del *Drupal* (soprattutto nella sezione di *back-end*).

La pagina per la registrazione online dei futuri associati CRUA è raggiungibile all'indirizzo:

https://www.crua.univpm.it/node/340#overlay-context=node/62

È stato possibile strutturare questa pagina dopo aver fatto una prima analisi sulla tipologia di dati che vengono inseriti in fase di iscrizione (appartenenti alla categoria di "rilascio volontario"), poiché l'analisi permette di inquadrare subito quali norme richiamare dal Regolamento e di studiare come applicarle nel caso specifico.

Successivamente, nel concepire la struttura del *database*, raggiunta la consapevolezza che l'applicazione non avrebbe richiesto considerevoli risorse a livello di contenuto e gestione dei dati, si è pensato di utilizzare la libreria *software SQLite*, versatile e di dimensione contenuta. L'ambiente di sviluppo scelto è il *PHP*, compatibile con i server che ospitano il sito del CRUA.

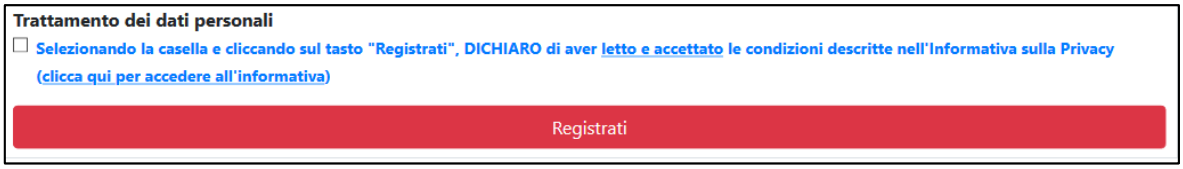
Inoltre, al fine di ridurre il lavoro per la realizzazione delle interfacce grafiche, si è pensato di usare la quarta versione del *framework css* "*Bootstrap"* (https://getbootstrap.com/), senza applicare modifiche al codice sorgente. Per l'impostazione grafica del *web-form* e delle diciture relative ai campi di input, sono stati presi a modello altri *web-form* di siti realmente esistenti. [29-42]

La struttura del *web-form*, divisa nelle sezioni di *front-end* e di *back-end*, viene di seguito descritta nel dettaglio.

### 2.1.1. FRONT-END

*Home-page*. È concepita in modo da presentare, all'utente che vuole iscriversi al Circolo, un *form* in cui può inserire i suoi dati personali. Ogni campo di input nel form è soggetto a un controllo *javascript* che ne rende obbligatoria la compilazione. Tra i vari campi di input si evidenzia quello relativo alla selezione delle attività di interesse, tramite apposizione di "spunta" sulle caselle di tipo *checkbox* (si veda APPENDICE - sezione FE, funzione n.1).

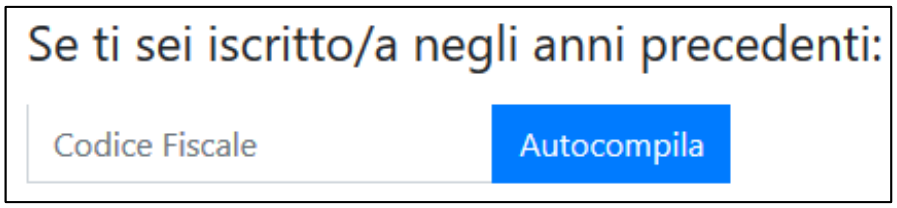
Terminata la compilazione di tutti i campi, per completare la registrazione l'utente deve cliccare sulla casella "Selezionando la casella e cliccando sul tasto "Registrati", DICHIARO di aver letto e accettato le condizioni descritte nell'Informativa sulla *Privacy* (clicca qui per accedere all'informativa)" apponendovi una spunta, nel caso in cui accetti le condizioni dell'informativa sulla *privacy* che può e deve consultare cliccando sulla scritta relativa (si veda APPENDICE - sezione FE, funzione n.5). Dopo aver cliccato sul tasto "Registrati", viene impedita qualsiasi ulteriore interazione con esso, al fine di evitare errori dovuti a eventuali ripetizioni dell'azione.



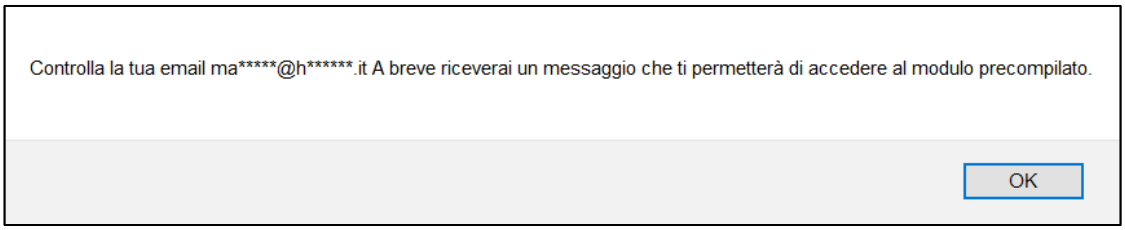

La registrazione prosegue soltanto se se ne accettano le condizioni ed è per questo motivo che in questa operazione sta il fulcro di tutta l'iscrizione: in questa fase l'utente fornisce effettivamente il consenso al trattamento dei dati personali per le finalità descritte nell'informativa da parte del titolare al trattamento (in questo caso il CRUA).

Dopo che l'utente avrà apposto la spunta alla casella e cliccato sul tasto "Registrati", la data e l'ora dell'azione verranno registrate nel database,

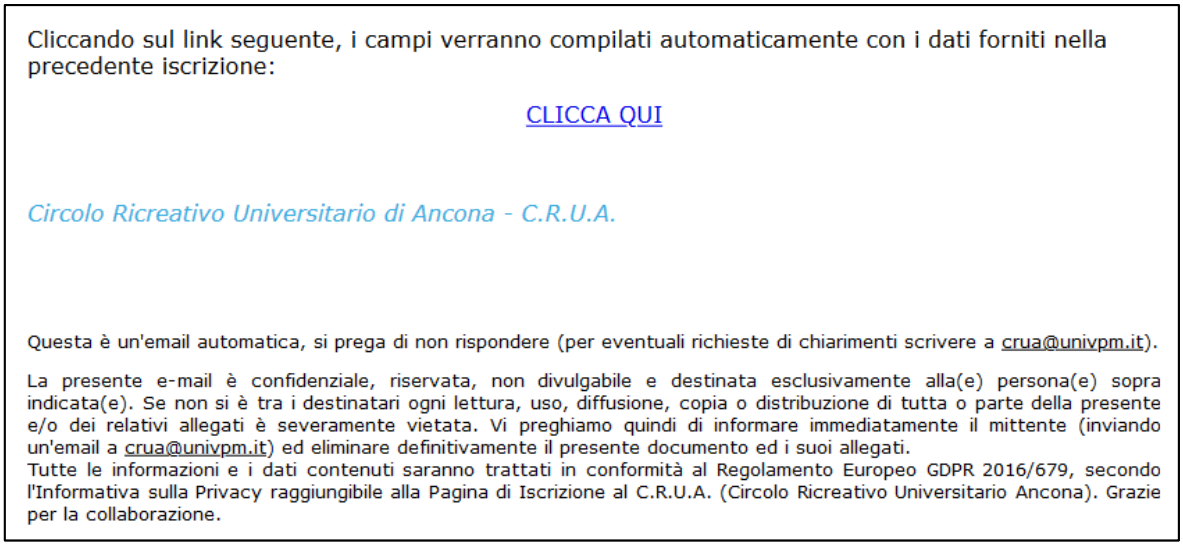
come prova del rilasciato consenso (si veda APPENDICE - sezione FE, funzione n.3).
Qualora l'utente si fosse iscritto in anni precedenti, questi ha anche la possibilità di compilare in modo automatico parte dei campi inserendo, nella sezione apposita, il suo codice fiscale (si veda APPENDICE - sezione FE, funzione n.4).




Cliccando poi sul bottone "Autocompila" viene inviato un messaggio, il cui invio è segnalato da un *alert* in cui viene indicato l'indirizzo *e-mail*, parzialmente oscurato per evitare che qualcuno a conoscenza del codice fiscale dell'interessato non arrivi ad apprenderne anche l'indirizzo *e-mail*. Allo stesso tempo, l'utente in regola può identificare l'indirizzo *e-mail* inserito in sede di iscrizione precedente, nel caso in cui non lo ricordasse.




Nel messaggio l'utente troverà un collegamento alla pagina CRUA dalla validità temporanea e costituito da una sequenza di caratteri alfanumerici casuali, che gli permette di accedere nuovamente alla pagina iniziale, stavolta compilata quasi interamente. La sequenza viene associata all'utente già presente nel database nel momento in cui viene cliccato il bottone "autocompila": il sistema dunque controlla che la sequenza esista e, in caso positivo, richiama i dati del socio e cancella la sequenza dal database.


Cliccando sul link seguente, i campi verranno compilati automaticamente con i dati forniti nella precedente iscrizione:

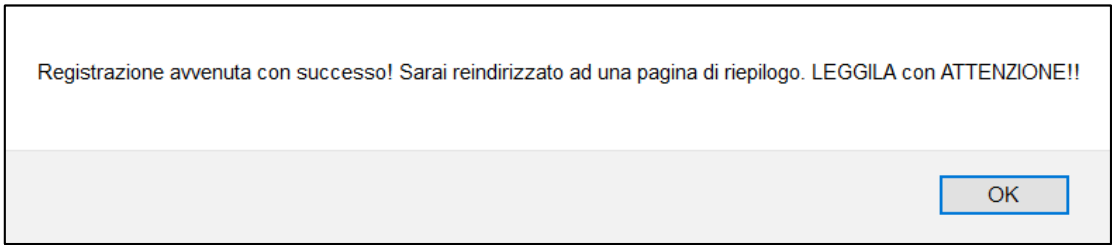
CLICCA QUI

*Circolo Ricreativo Universitario di Ancona - C.R.U.A.*

Questa è un'email automatica, si prega di non rispondere (per eventuali richieste di chiarimenti scrivere a crua@univpm.it).

La presente e-mail è confidenziale, riservata, non divulgabile e destinata esclusivamente alla(e) persona(e) sopra indicata(e). Se non si è tra i destinatari ogni lettura, uso, diffusione, copia o distribuzione di tutta o parte della presente e/o dei relativi allegati è severamente vietata. Vi preghiamo quindi di informare immediatamente il mittente (inviando un'email a crua@univpm.it) ed eliminare definitivamente il presente documento ed i suoi allegati.
Tutte le informazioni e i dati contenuti saranno trattati in conformità al Regolamento Europeo GDPR 2016/679, secondo l'Informativa sulla Privacy raggiungibile alla Pagina di Iscrizione al C.R.U.A. (Circolo Ricreativo Universitario Ancona). Grazie per la collaborazione.

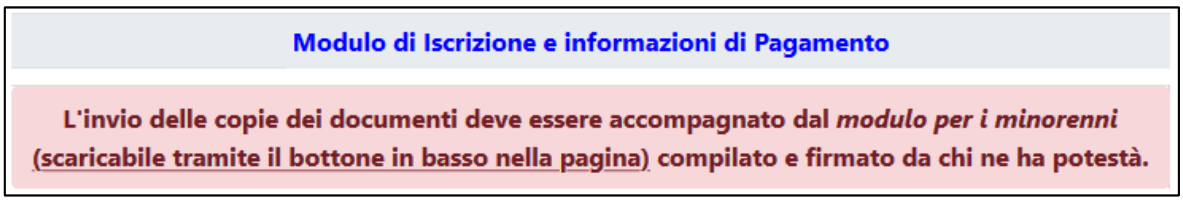
Completata la compilazione, apposta la spunta alla casella relativa al rilascio del consenso dei dati personali e cliccato il tasto "Registrati", l'utente viene avvisato da un *alert* che sta per essere reindirizzato ad una pagina di riepilogo dei dati inseriti.




La pagina di riepilogo verso cui si viene reindirizzati (rif. capitolo 3, *screenshot* n.5 e n.6) ha una sezione "fissa" in alto, in cui vengono visualizzati tutti i dati inseriti dall'utente nell'*home-page* e una parte in basso dove può visualizzare le informazioni per il pagamento.
Il testo presente in quest'ultima sezione ("Modulo di Iscrizione e Informazioni di Pagamento") cambia a seconda del metodo di pagamento selezionato (Bonifico o Addebito su busta paga) e della categoria del socio (Esterno o Affiliato UNIVPM).
Infatti, l'utente può visualizzare le informazioni sul metodo di pagamento scelto e le modalità per effettuarlo ed ha la possibilità di scaricare i moduli di consenso all'iscrizione da firmare e inviare via *e-mail* oltre che di

stampare la pagina di riepilogo per controllare che i dati siano stati inseriti correttamente. Nel caso egli riscontrasse qualche errore può richiedere la rettifica dei dati al titolare del trattamento, grazie al "diritto di rettifica".
La suddetta pagina di riepilogo è raggiungibile tramite un indirizzo generato al momento del completamento dell'operazione di registrazione, tramite un algoritmo che a sua volta genera caratteri alfanumerici casuali (comunque conformi a un determinato schema).
In un primo momento del progetto, il *link* era costituito da una sequenza di numeri e lettere la cui semplice sostituzione con i valori del numero identificativo e del numero della tessera di un altro possibile associato avrebbe portato alla visualizzazione dei dati di quest'ultimo.
Si precisa che al *click* del tasto "Registrati", viene anche inviata un'" *e-mail* di benvenuto" (personalizzata per ogni combinazione di tipologia utente/pagamento scelto – rif. capitolo 3, *screenshot* n.4) al nuovo associato in cui gli vengono ricordati gli adempimenti che gli mancano per completare l'iscrizione e in cui è riportato un *link* alla pagina di riepilogo dei dati, per permettergli, qualora non lo avesse fatto, di ricontrollare i dati inseriti (che però non potrà modificare) e scaricare i moduli da compilare e firmare.
Qualora l'utente iscritto abbia un'età inferiore ai quattordici anni, la pagina di riepilogo riporterebbe una dicitura apposita evidenziata in un riquadro dallo sfondo di colore rosso che richiede di inviare il documento di identità del genitore e il modulo di autorizzazione all'iscrizione del minore compilato e firmato. Infatti, nel campo dell'*home-page* in cui si inserisce la data di nascita, viene effettuato un controllo sull'età attraverso il calcolo della differenza tra la data dell'iscrizione e quella di nascita dell'utente (si veda APPENDICE - sezione FE, funzione n.2). Quest'ultimo è informato in prima battuta di un'occorrenza insolita proprio nell'*home-page*, poiché sotto al campo dell'*e-mail* viene riportata la dicitura "In caso di minorenne con età inferiore a 14 anni, va indicata l'*e-mail* del genitore".

In questo modo l'*e-mail* di richiesta del modulo con il consenso da firmare, viene indirizzata e rivolta direttamente al genitore.



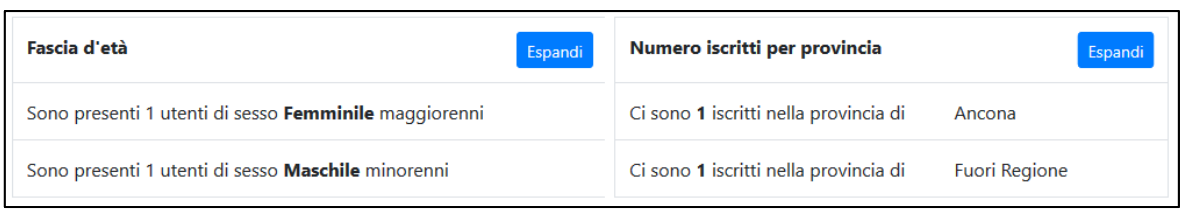

### 2.1.2. BACK-END

Il *back-end* è la sezione destinata al titolare e al responsabile del trattamento dati: vi si accede tramite una pagina di login e si presenta all'utente collegato con una pagina in cui è possibile scegliere in quale sottosezione entrare tra "Libro Soci", "Opzioni *Login*", "Impostazione *PDF*" e "*Backup* Dati".

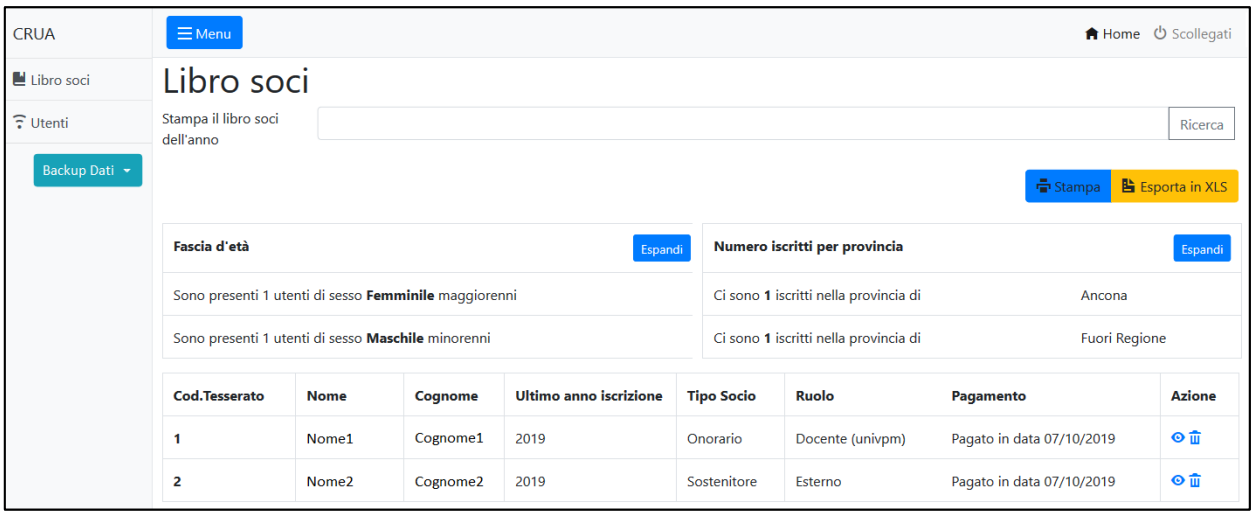
La sottosezione principale è "Libro Soci" ed è possibile scegliere quale funzione utilizzare tra:

1. Visualizzazione delle statistiche relative a quell'anno;
2. Visualizzazione/Stampa dei nominativi iscritti nell'anno di riferimento;
3. Visualizzazione/Modifica/Cancellazione singole schede utente;
4. Cambio dell'anno di riferimento.

1) Cliccando sui relativi bottoni "Espandi" è possibile vedere quanti iscritti di sesso maschile o femminile maggiorenni o minorenni ci sono per quell'anno di riferimento e quanti iscritti risiedono in ogni provincia marchigiana oppure quanti di loro risiedono nelle altre regioni italiane.



2) È possibile visualizzare l'elenco di tutti gli iscritti nell'anno di riferimento e controllare velocemente le caratteristiche principali, di cui Codice Tessera, Nome e Cognome, Ultimo anno di iscrizione, Tipo di socio (ordinario o sostenitore [2]), Ruolo, Stato del pagamento. Inoltre, si può stampare l'elenco oppure esportarlo nel formato *XLS* (cioè compatibile, ad esempio, con i programmi *Microsoft Excel o LibreOffice Calc*) grazie ai bottoni appositi (si veda APPENDICE - sezione BE, funzione n.5).

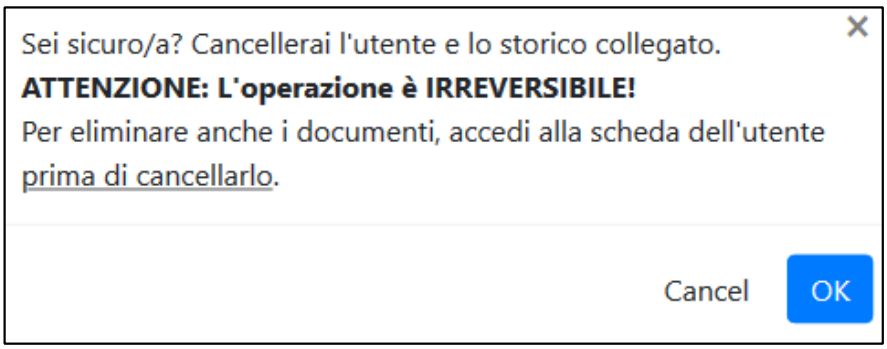



3) Tramite il *click* sulle piccole icone situate a fianco di ogni nominativo, è possibile visualizzare la scheda singola di ogni utente iscritto oppure cancellarne definitivamente tutti i dati (si veda APPENDICE - sezione BE, funzione n.4).

| Cod.Tesserato | Nome | Cognome | Ultimo anno iscrizione | Tipo Socio | Ruolo | Pagamento | Azione |
|---|---|---|---|---|---|---|---|
| 1 | Nome1 | Cognome1 | 2019 | Onorario | Docente (univpm) | Pagato in data 07/10/2019 | |
| 2 | Nome2 | Cognome2 | 2019 | Sostenitore | Esterno | Pagato in data 07/10/2019 | |

Nel caso in cui pervenisse la revoca dell'iscrizione al CRUA, per eliminare i dati e lo storico di un iscritto è sufficiente cliccare sull'icona della cancellazione a fianco del nominativo ma, per eliminare i documenti ad esso collegati, è necessario effettuare un passaggio di cancellazione

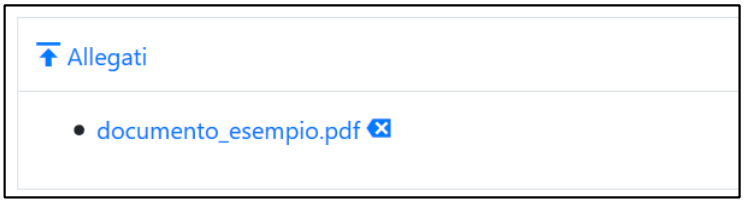
manuale dei documenti ed in questo caso un *alert* illustra all'utente la corretta procedura da seguire.




Entrando in modalità di visualizzazione della singola scheda del tesserato (rif. capitolo 3, *screenshot* n.11), è possibile anche modificarne i dati intervenendo sulla scheda generica del tesserato (nella parte superiore della pagina) oppure sulla scheda relativa al singolo anno di iscrizione (si veda APPENDICE - sezione BE, funzione n.6). Questa distinzione è stata attuata per permettere l'applicazione del diritto di rettifica descritto nell'art. 16 del Regolamento UE 679/2016 (tramite la modifica della scheda generica) e per confrontare (con la scheda annuale) i dati relativi agli anni precedenti.

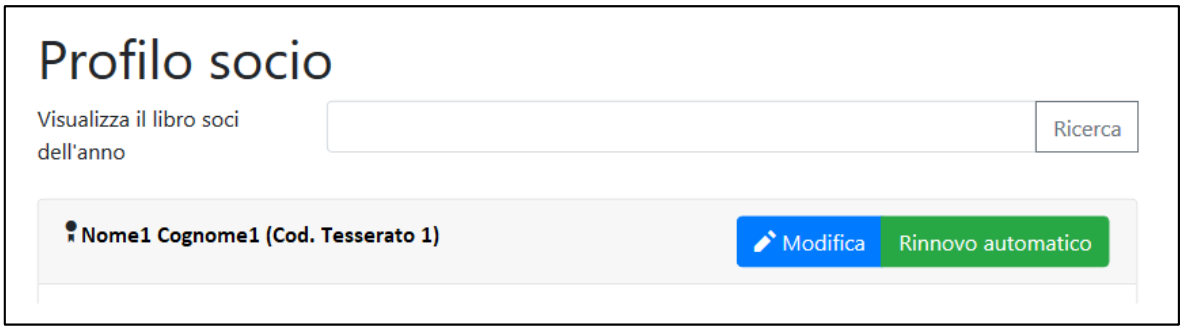
È inoltre possibile effettuare l'*upload* dei documenti (esclusivamente in formato *pdf*) che l'associato è tenuto ad inviare tramite *e-mail* una volta completato l'inserimento dei dati in fase di iscrizione, tra i quali figurano il modulo di adesione firmato, la ricevuta del bonifico bancario ed eventualmente il modulo di autorizzazione per l'iscrizione del minorenne compilato e firmato (si veda APPENDICE - sezione BE, funzione n.8). Cliccando sul nome del documento, è possibile visualizzarlo inserendo, in fase di apertura dello stesso, la *password* precedentemente impostata dall'/dagli amministratore/i (si veda APPENDICE - sezione BE, funzione n.7); se ci fosse l'esigenza di eliminare il *file*, magari in caso di erroneo inserimento o in caso di richiesta esplicita dell'associato, cliccando sull'icona apposita (situata a fianco del documento) è possibile cancellare il documento.

Quando il file *pdf* viene caricato, è salvato "fisicamente" in una sottocartella apposita (dedicata al tesserato e chiamata con il suo numero di tessera) che si crea e colloca, automaticamente all'atto di caricamento del file stesso, all'interno delle *directory* "webformcrua/associato" (precisamente in un'ulteriore sottocartella avente, come nome, l'anno del caricamento - si veda APPENDICE - sezione BE, funzione n.3).
Per far sì che le sottocartelle relative al numero di tessera (create automaticamente dall'*upload* di *file pdf*) siano ordinate correttamente, è stata inserita la funzione *php* "str_pad_left" che aggiunge tanti zeri al numero originario della tessera quanti ne servono per arrivare a 7 cifre totali.



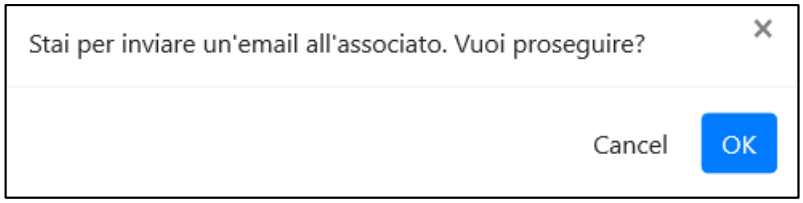

Nella prima fase di progetto del *web-form* si era pensato di permettere l'upload dei *file* direttamente agli utenti che vogliono iscriversi (per evitare loro l'invio successivo dei documenti via *e-mail*), ma l'idea non è stata concretizzata perché avrebbe esposto l'intero sistema ad un rischio elevatissimo di attacco da parte di malintenzionati. Tra l'altro, la modifica avrebbe richiesto anche la creazione di un'area riservata in *back-end* per ogni utente, in modo da poter risalire all'autore di un eventuale attacco "dall'interno".
Altre funzionalità accessibili, tramite bottoni appositi, nella visualizzazione della scheda singola dell'utente, sono il "rinnovo automatico" e l'"invia tessera".
La prima funzionalità serve all'amministratore come "promemoria": indica che il rinnovo del pagamento avviene in modo automatico (per ora riguarda l'addebito sulla busta paga, quindi usato solo per il Personale Tecnico Amministrativo e Docente dell'Università Politecnica delle

Marche) e non necessita dell'intervento manuale e annuale dell'iscritto; infatti quando l'opzione è attiva, il sistema copia i dati relativi alla scheda annuale (dell'anno corrente) nella tabella del database "associato_anno" e lo stato di pagamento cambia in "pagato" anche per l'anno successivo (se impostato in tal modo nell'anno corrente) con la data di pagamento impostata di default. Se il "rinnovo automatico" non è attivo, è necessario modificare lo stato del pagamento da "in attesa di pagamento" a "pagato" manualmente, inserendo la data di quando il pagamento è stato convalidato.




La seconda funzionalità serve a comunicare all'utente, tramite un'*e-mail* di conferma, l'avvenuta regolarizzazione dell'iscrizione e i dati che verranno riportati sulla sua tessera (rif. capitolo 3, *screenshot* n.12). Quest'ultima funzionalità è accessibile solo se il pagamento risulta convalidato.


Comunque, entrambi i bottoni sopra citati assumono un colore diverso a seconda dello stato di attivazione della relativa funzione: se attivato, il bottone assume colore verde (dopo un'ulteriore richiesta di conferma all'utente), altrimenti rimane di colore giallo.




4) Nella barra di ricerca è possibile inserire l'anno di cui si vogliono visualizzare gli iscritti.


In automatico, sulla pagina principale, viene visualizzato l'elenco relativo all'anno corrente. Cambiando l'anno di riferimento, è possibile usare tutte le funzioni presentate precedentemente anche sugli iscritti di un anno differente.

Per quanto riguarda la conservazione dei dati nel database, essa è regolamentata dal principio di conservazione riportato nell'art. 5 lett. e del Regolamento. Dunque, nel caso del sito CRUA, i dati vengono conservati fino alla (eventuale) revoca del consenso da parte dell'interessato.

Qualora al CRUA pervenisse una richiesta dell'utente di questo tipo, i dati dovranno essere cancellati completamente o in alternativa potranno essere conservati, magari per fini statistici (e.g. quanti iscritti sono residenti in/fuori regione, quanti sono di sesso maschile/femminile, quanti sono minorenni/maggiorenni), a patto di essere resi "anonimi" (es. attraverso la modifica del nome e del cognome in generici "Nome" e "Cognome" e la rimozione del codice fiscale) e quindi non più riconducibili all'utente originario. È anche vero però, che "la revoca del consenso non pregiudica la liceità del trattamento basato sul consenso prima della revoca" (art. 7, par. 3 Regolamento UE 679/2016).

Dunque, sebbene "il consenso possa essere revocato con la stessa facilità con cui può essere accordato" da parte dell'Interessato (in qualsiasi momento), il CRUA potrà conservare i documenti degli iscritti relativi alle annualità precedenti la revoca "se esistono motivi legittimi cogenti che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato e se servono all'accertamento, all'esercizio o alla difesa di un diritto in sede giudiziaria" (art. 21, par. 1 Regolamento UE 679/2016).

In "Opzioni Login" si possono inserire nuovi amministratori o modificare le credenziali (username e *password*) di quelli esistenti, ovvero dei titolari o dei responsabili al trattamento dati che avranno accesso alla sezione di *back-end* (e quindi ai dati degli iscritti - si veda APPENDICE - sezione BE, funzione n.2).
Se si vuole cambiare la *password* di un amministratore già inserito è sufficiente scriverla nel campo apposito e poi puntare e cliccare con il cursore in una zona vuota della pagina. A quel punto comparirà un piccolo messaggio che confermerà l'aggiornamento della *password*.


In "Impostazione *PDF*" è possibile impostare una *password* per la protezione dei documenti caricati in "*Upload* Allegati" (all'interno delle schede degli iscritti) prima che avvenga l'*upload* degli stessi. Questa funzionalità è stata implementata per proteggere ulteriormente i documenti in caso di *data breach,* insieme alla pseudonimizzazione che il

responsabile al trattamento dovrà applicare. Infatti, qualora dovesse occorrere una violazione dei dati, i file degli utenti sarebbero protetti da *password* e senza conoscerla non si riuscirebbe ad aprirli, pur essendo riusciti ad accedervi.

In una prima costruzione del sito si era pensato di introdurre anche il caricamento del documento di identità dell'associato (per verificare che non avesse dichiarato dati falsi), ma, per risultare conformi al principio della minimizzazione dei dati (art. 5, par. 1 lett. c del Regolamento UE 679/2016), l'idea è stata scartata.

L'amministratore può controllare in quale data l'ultima *password* è stata impostata e, se l'impostazione non è mai avvenuta, viene visualizzata la scritta "Mai impostata!".

Se la *password* venisse cambiata dopo che è stato già effettuato l'*upload* di file, la modifica si applicherebbe solo ai *file* caricati dopo la modifica stessa (per i *file* antecedenti la modifica rimarrebbe valida la *password* precedente). Non è stato possibile fare in modo che la nuova *password* venisse applicata anche ai documenti caricati precedentemente perché le operazioni di ricerca dei *file* e di applicazione della *password* avrebbero richiesto un intervallo tempo non sostenibile da un processo *php web* (che ha un tempo di esecuzione massimo di 30 secondi).


In "*Backup* Dati" si può scegliere se effettuare una copia di sicurezza attraverso il *backup* immediato (che permette di scaricarla sul

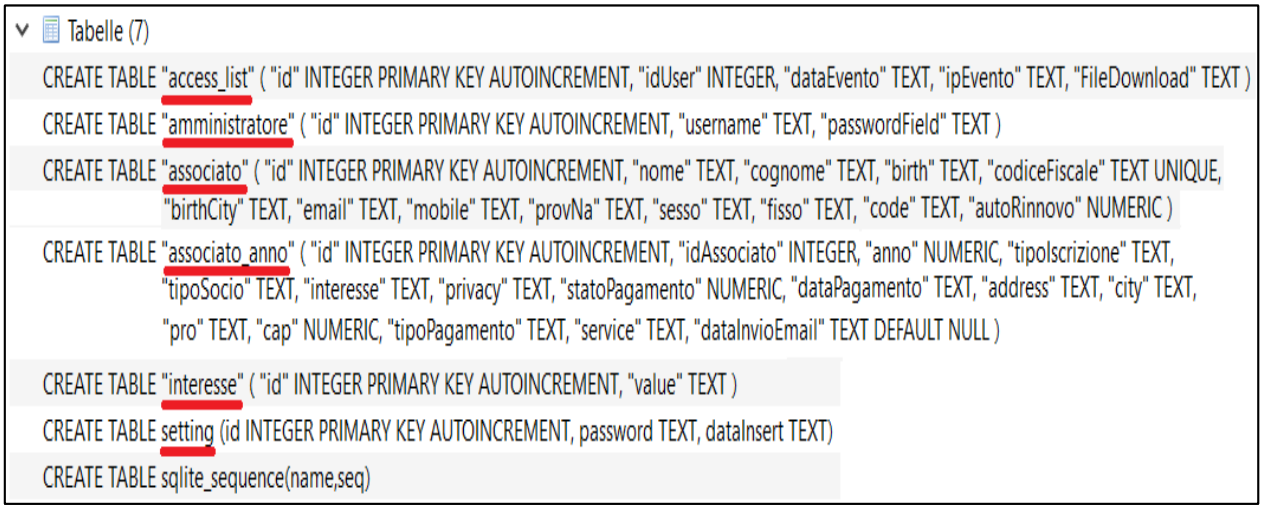
proprio dispositivo) oppure attraverso il salvataggio sul proprio dispositivo di una copia tra quelle effettuate in automatico dal sistema una volta ogni tre mesi (si veda APPENDICE - sezione BE, funzione n.1). Il sistema infatti conserva, senza sovrascriverli, fino a quaranta *file* di *backup* automatici, ovvero relativi ad un arco temporale di dieci anni).


### 2.1.3. STRUTTURA DEL DATABASE

Tutti i dati inseriti dai futuri associati vengono registrati in un *database* in formato *SQLite* composto da sei tabelle (più una, la "sqlite_sequence", creata automaticamente):

1) "access_list" per registrare l'identità e la data/ora dell'accesso ai documenti *pdf* caricati in *back-end* (relativi ai singoli iscritti);
2) "amministratore" per le credenziali degli utenti che possono accedere al *back-end*;
3) "associato" per l'elenco dell'*id*, del nome/cognome, data di nascita, codice fiscale, città/provincia di nascita, *e-mail*, numero di telefono cellulare/fisso e il genere;
4) "associato_anno" per l'*id* associato, l'anno di iscrizione, il tipo di iscrizione, il tipo di socio e gli interessi (a ogni numero corrisponde una tipologia), la data e l'ora in cui è stato fornito il consenso al trattamento dei dati, lo stato e la data del pagamento, l'indirizzo di residenza, il tipo di pagamento selezionato, la struttura in cui si lavora (solo per PTA e docenti univpm) e la data in cui si è inviata l'*e-mail* con la tessera d'iscrizione all'associato;

5) "interesse" per attribuire a ogni attività un numero (es. 1= podismo, 2= pesca, ecc.);
6) "setting" per le impostazioni dei documenti *pdf* caricati in *back-end*.

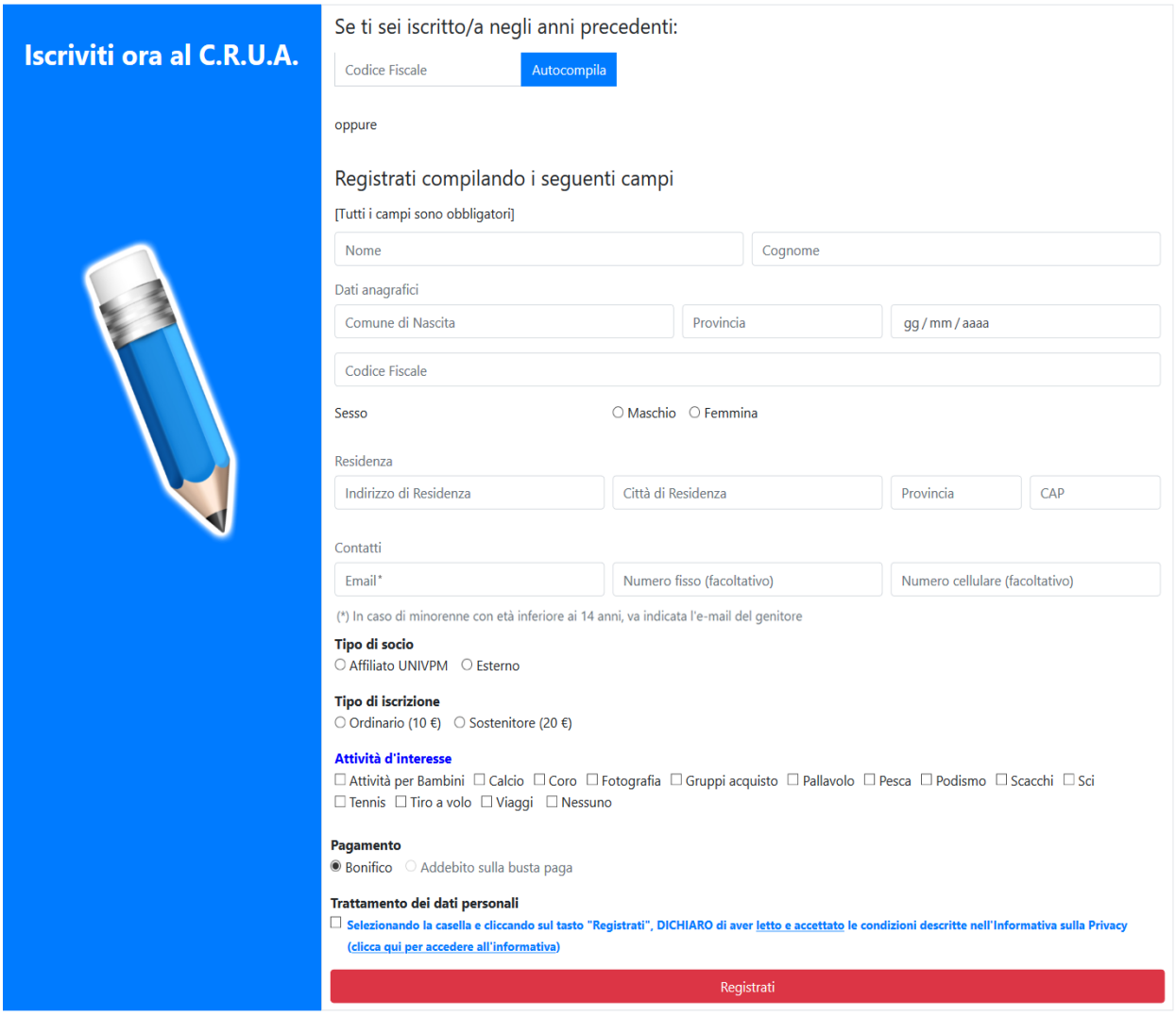


# 3. IMPLEMENTAZIONE DEL SITO

Il *web-form* CRUA si compone di 14 *file* sorgenti in formato *php* e di 5 *file* sorgenti in formato *html*. Questi ultimi contengono il testo con la relativa formattazione (impostazione grafica) dell'*e-mail* a cui il codice in *php* fa riferimento in alcune sezioni.

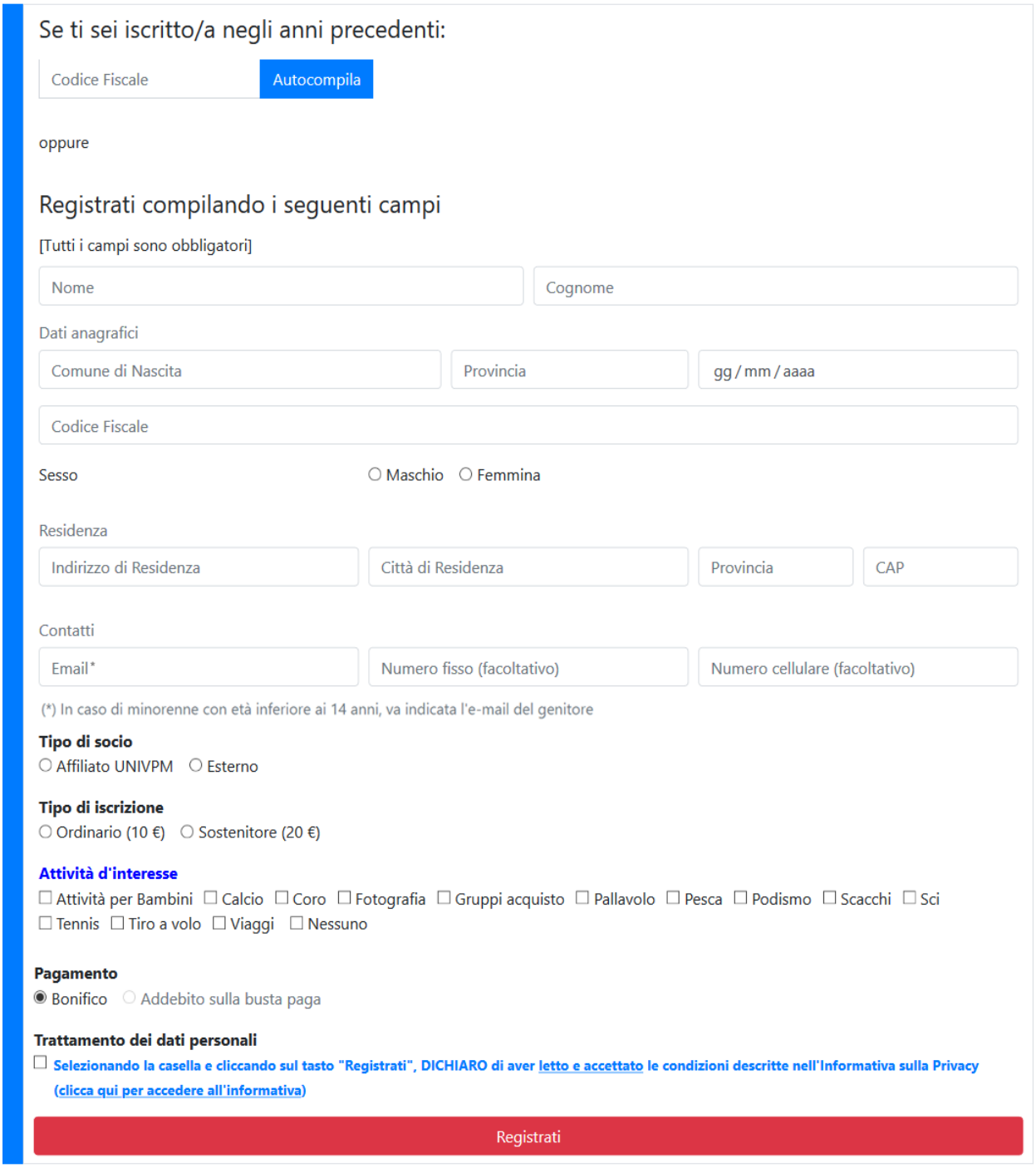
Inoltre, nelle cartelle "resources" e "vendor", sono presenti tutte le risorse, scaricate sul sistema per evitare il collegamento "all'esterno" ogni qualvolta che si accede al *web-form*.

Di seguito vengono riportati alcuni *screenshot* del *web-form* per l'iscrizione degli utenti, in ordine di apparizione delle pagine *web*.



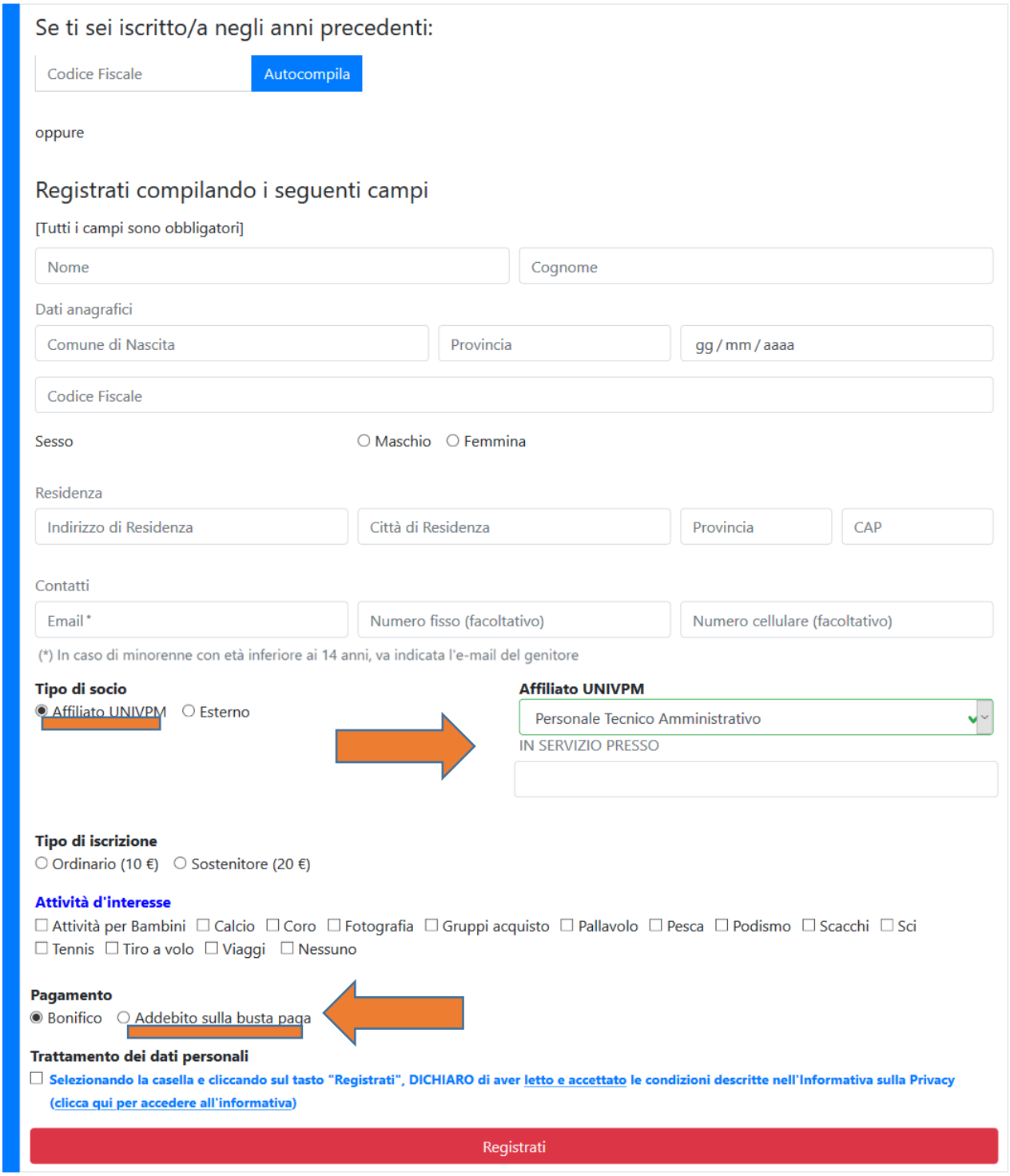
*Front-end:*

*Screenshot n.1. Home-page - Form di iscrizione* [I]




*Front-end:*

*Screenshot n.2. Home-page - Form di iscrizione, dettaglio* [I]




*Front-end:*

*Screenshot n.3. Home-page - Il radio-button "Addebito sulla busta paga" è sempre visibile, ma è attivo e selezionabile soltanto se si sceglie la voce "Affiliato UNIVPM" e successivamente "Docente" oppure "Personale Tecnico Amministrativo".* [I]

Benvenuto/a nel **Circolo Ricreativo Universitario di Ancona**!

La prima fase della procedura di iscrizione è andata a buon fine.

Per completare l'iscrizione dovrai inviare il modulo scaricato nella schermata di riepilogo compilato e firmato, insieme alla ricevuta del bonifico, all'indirizzo **crua@univpm.it**

Qualora non avessi effettuato il download dei moduli da compilare e firmare, puoi riaccedere alla pagina di riepilogo della tua iscrizione cliccando QUI.

*Circolo Ricreativo Universitario di Ancona - C.R.U.A.*

Questa è un'email automatica, si prega di non rispondere (per eventuali richieste di chiarimenti scrivere a crua@univpm.it).

La presente e-mail è confidenziale, riservata, non divulgabile e destinata esclusivamente alla(e) persona(e) sopra indicata(e). Se non si è tra i destinatari ogni lettura, uso, diffusione, copia o distribuzione di tutta o parte della presente e/o dei relativi allegati è severamente vietata. Vi preghiamo quindi di informare immediatamente il mittente (inviando un'email a crua@univpm.it) ed eliminare definitivamente il presente documento ed i suoi allegati.
Tutte le informazioni e i dati contenuti saranno trattati in conformità al Regolamento Europeo GDPR 2016/679, secondo l'Informativa sulla Privacy raggiungibile alla Pagina di Iscrizione al C.R.U.A. (Circolo Ricreativo Universitario Ancona). Grazie per la collaborazione.

*E-mail:*

*Screenshot n.4. Messaggio di benvenuto, inviato all'iscritto dopo il clic su "Registrati".*


**Riepilogo dati - Tesserato N. 0000001**

| | | | |
|---|---|---|---|
| **Nome** | Nome | **Cognome** | Cognome |
| **Data di nascita** | 01-01-1901 | **Luogo di nascita** | Ancona |
| **Codice Fiscale** | CODICEFISCALE1234 | | |
| **E-mail** | esempio@esempio.it | **Telefono fisso:** | 0987654321 |
| | | **Telefono mobile:** | 1234567890 |
| **Indirizzo** | Via dei Fiori - 61234 Ancona | | |
| **Tipo di socio** | Esterno | **Tipo di iscrizione** | Ordinario |
| | | **Costo iscrizione** | 10 € |
| **Interessi:** | Calcio, Pesca, Scacchi, Tennis | | |
| **Tipo pagamento** | Bonifico | **Stato pagamento** | In attesa |

**Modulo di Iscrizione e informazioni di Pagamento**

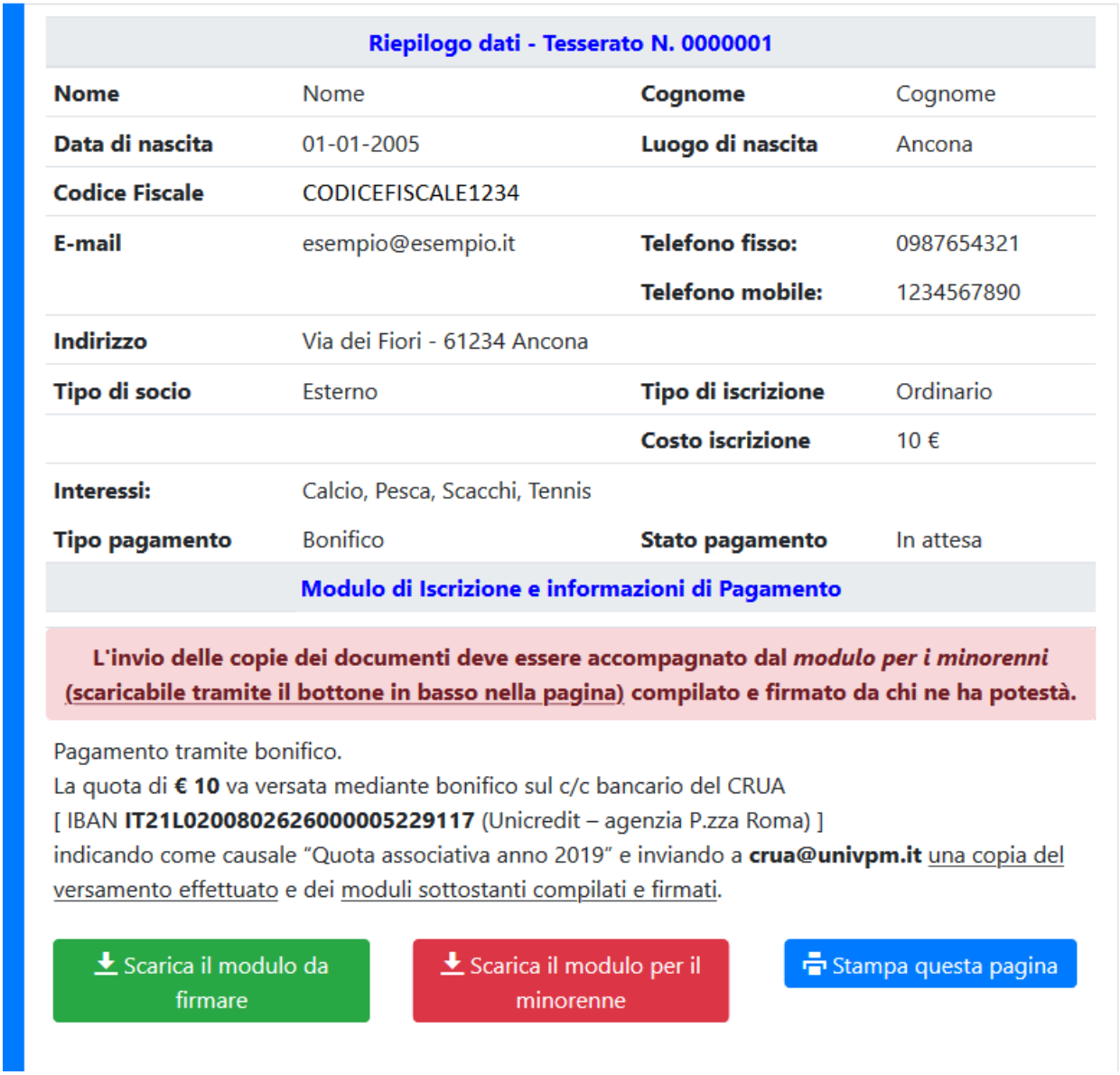
Pagamento tramite bonifico.
La quota di **€ 10** va versata mediante bonifico sul c/c bancario del CRUA
[ IBAN **IT21L0200802626000005229117** (Unicredit – agenzia P.zza Roma) ]
indicando come causale "Quota associativa anno 2019" e inviando a **crua@univpm.it** una copia del versamento effettuato e del modulo sottostante firmato.

Scarica il modulo da firmare

Stampa questa pagina

*Front-end:*

*Screenshot n.5. Pagina di Riepilogo dati (ci si viene reindirizzati dopo l'accettazione dei dati inseriti in Home-page).* [II]



**Riepilogo dati - Tesserato N. 0000001**

| | | | |
|---|---|---|---|
| **Nome** | Nome | **Cognome** | Cognome |
| **Data di nascita** | 01-01-2005 | **Luogo di nascita** | Ancona |
| **Codice Fiscale** | CODICEFISCALE1234 | | |
| **E-mail** | esempio@esempio.it | **Telefono fisso:** | 0987654321 |
| | | **Telefono mobile:** | 1234567890 |
| **Indirizzo** | Via dei Fiori - 61234 Ancona | | |
| **Tipo di socio** | Esterno | **Tipo di iscrizione** | Ordinario |
| | | **Costo iscrizione** | 10 € |
| **Interessi:** | Calcio, Pesca, Scacchi, Tennis | | |
| **Tipo pagamento** | Bonifico | **Stato pagamento** | In attesa |

**Modulo di Iscrizione e informazioni di Pagamento**

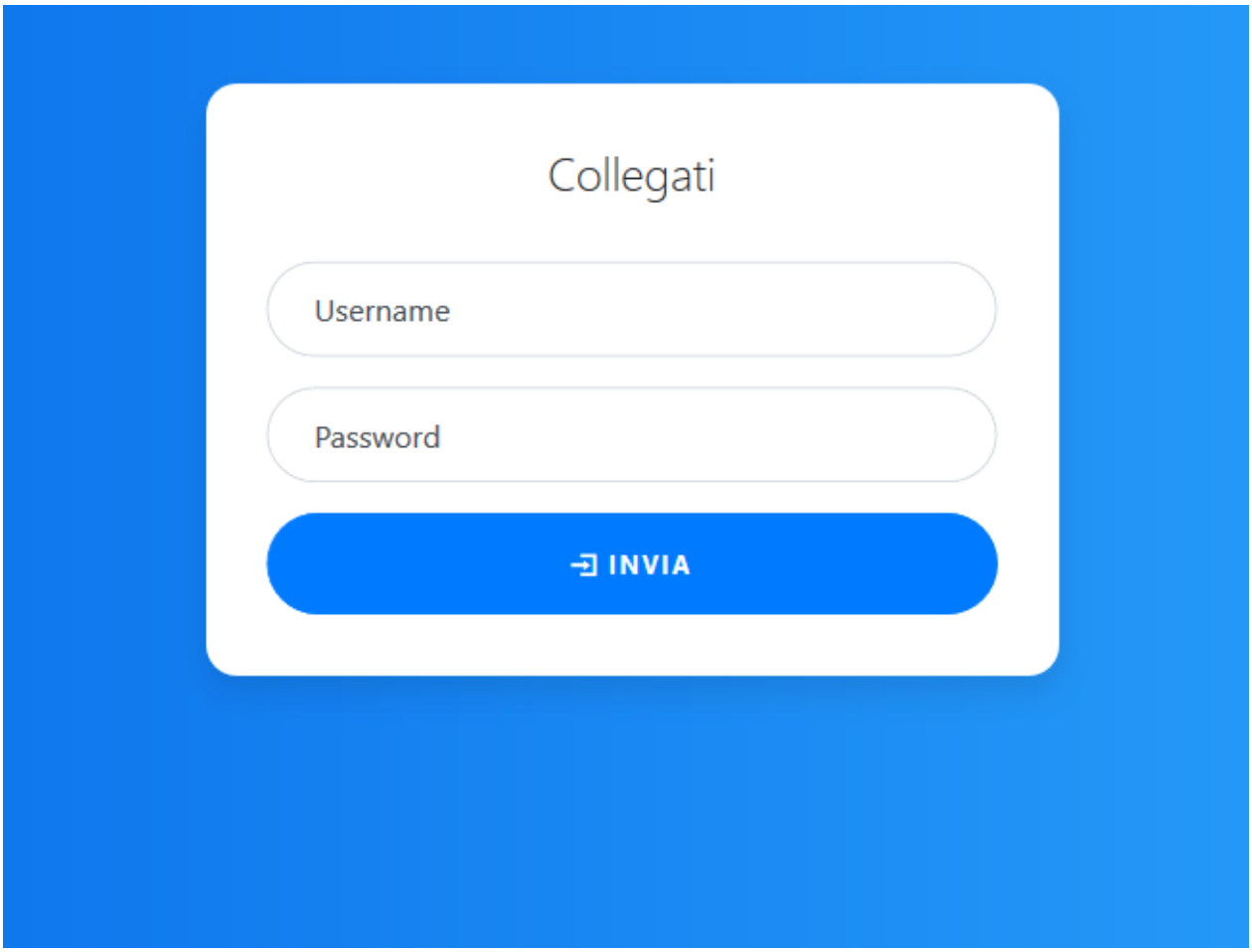
**L'invio delle copie dei documenti deve essere accompagnato dal *modulo per i minorenni* (scaricabile tramite il bottone in basso nella pagina) compilato e firmato da chi ne ha potestà.**

Pagamento tramite bonifico.
La quota di **€ 10** va versata mediante bonifico sul c/c bancario del CRUA
[ IBAN **IT21L0200802626000005229117** (Unicredit – agenzia P.zza Roma) ]
indicando come causale "Quota associativa anno 2019" e inviando a **crua@univpm.it** una copia del versamento effettuato e dei moduli sottostanti compilati e firmati.

Scarica il modulo da firmare | Scarica il modulo per il minorenne | Stampa questa pagina

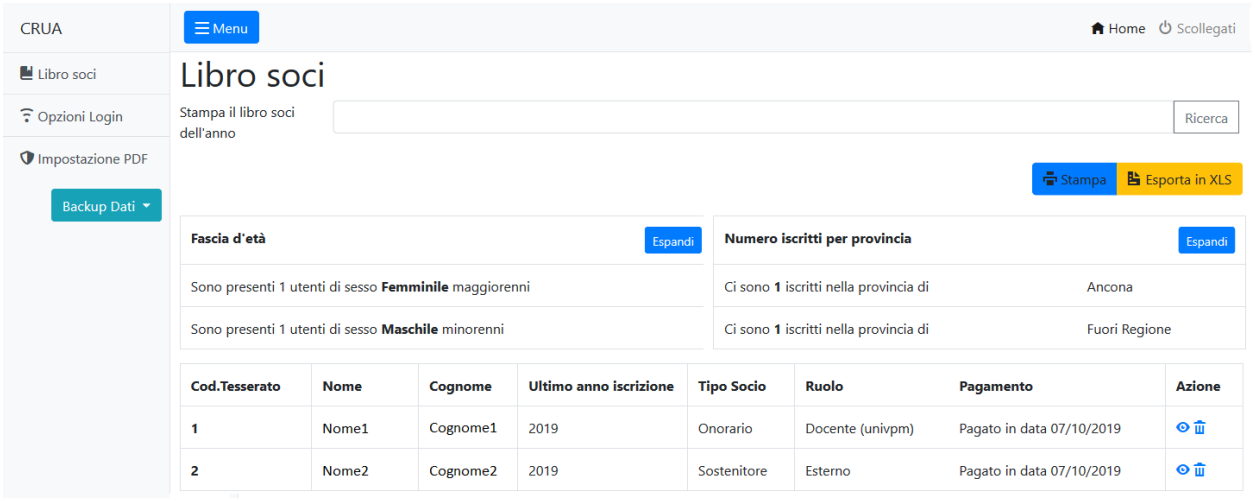
*Front-end:*

*Screenshot n.6. Pagina di Riepilogo dati (caso di iscritto minorenne), dettaglio.* [II]



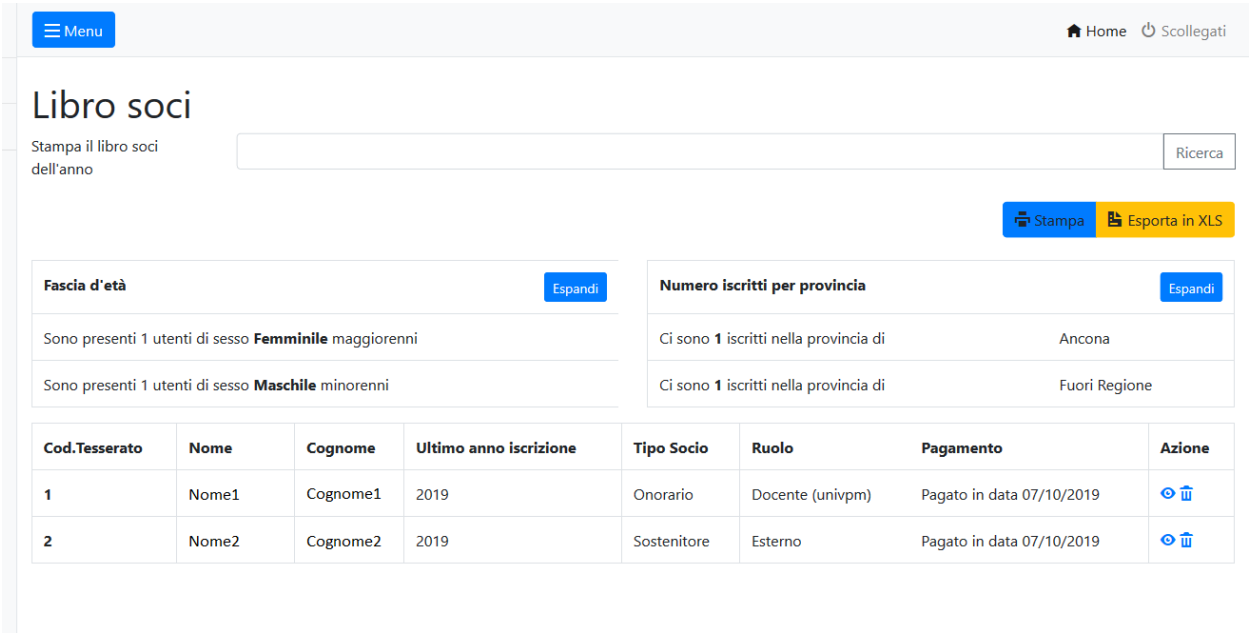

*<u>Pagina di login:</u>*

*Screenshot n.7. Destinata a chi tratta i dati degli iscritti, per accedere al back-end.* [VI]



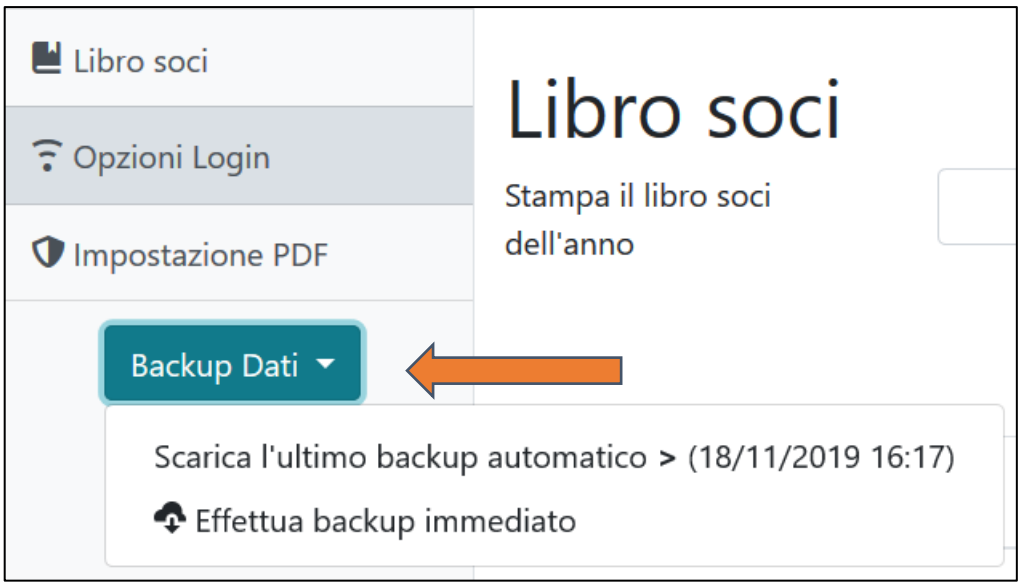

*<u>Back-end:</u>*

*Screenshot n.8. Area accessibile dopo aver effettuato il login.* [VI, VIII]



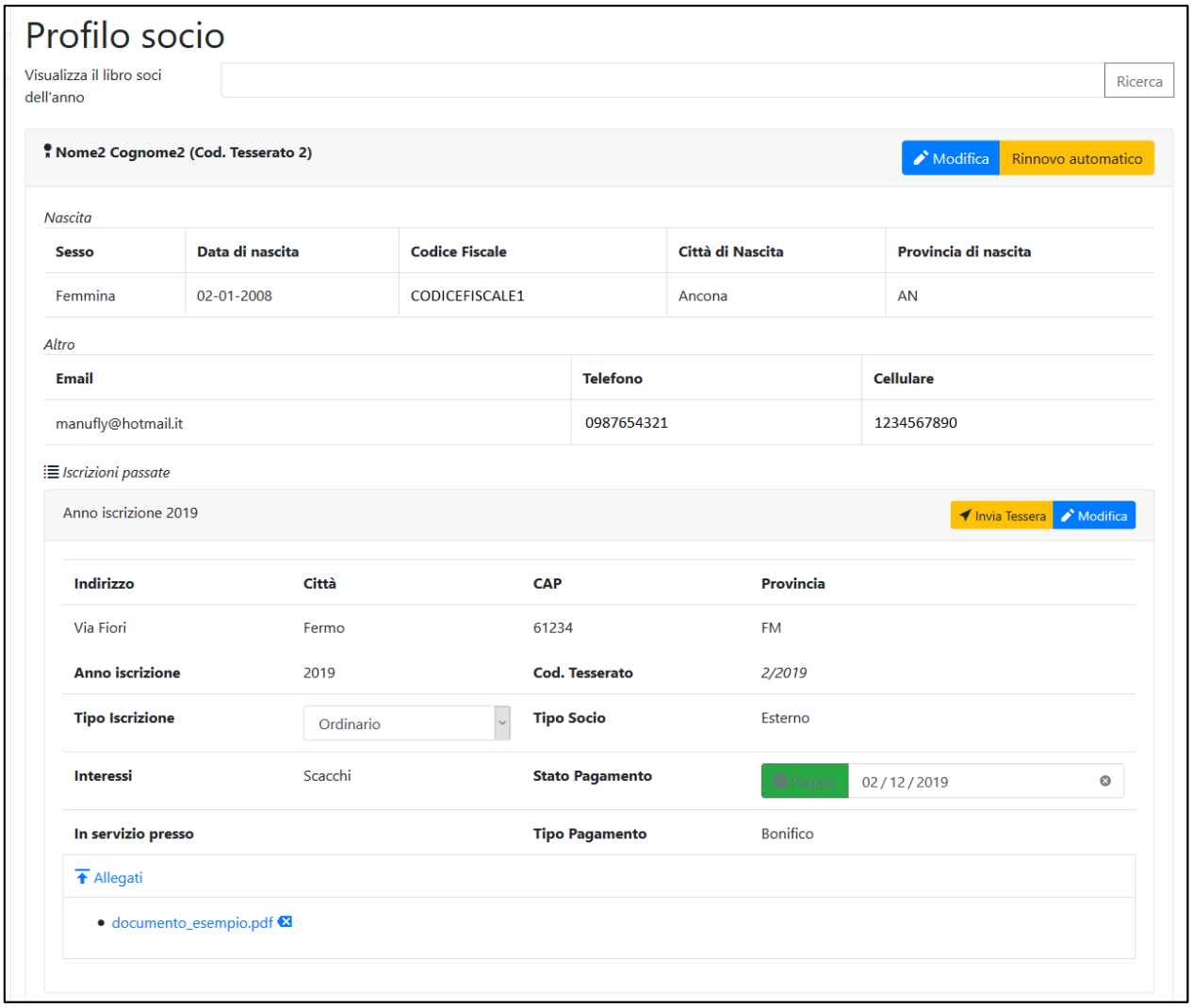

*<u>Back-end:</u>*

*Screenshot n.9. Area accessibile dopo aver effettuato il login, nel dettaglio.* [VI, VIII]




*<u>Back-end:</u>*

*Screenshot n.10. Dettaglio backup dati; con questo bottone è possibile scaricare l'ultimo backup effettuato automaticamente dal sistema una volta ogni tre mesi, oppure effettuarne uno in tempo reale.* [VIII]




*<u>Back-end:</u>*

*Screenshot n.11. Visualizzazione scheda utente, con dati modificabili e pannello di accesso agli allegati in basso (per caricare documenti sul sistema e, se presenti, visualizzarli/scaricarli).* [XII]


*E-mail:*

*Screenshot n.12. Messaggio inviato all'iscritto grazie alla funzione "Invia Tessera", presente nella scheda utente, con nome, cognome, numero della tessera e anno di validità compilati automaticamente.*

*La grafica del messaggio è generata dall'uso di un template generator, del sito https://beefree.io/editor/*

# 4. CONCLUSIONI E SVILUPPI FUTURI

A conclusione di questa tesi, è possibile dire che l'implementazione del sito del CRUA è stata effettuata in modo ottimale, rispettando sia le specifiche fornite dall'associazione, sia le tante e diverse norme introdotte dal GDPR che dovrebbero garantire la tutela dei dati personali nonché della *privacy* degli utenti, fin troppe volte messa a rischio dal mondo del *World Wide Web*.

Il Regolamento infatti promuove la responsabilizzazione dei titolari del trattamento, la detenzione del potere decisionale sul trattamento dei dati da parte dell'interessato, nonché l'adozione di politiche che prendano in considerazione, in modo continuo e costante, i rischi e i pericoli che, in occasione di determinate attività di trattamento di dati personali, possono gravare sui diritti e sulle libertà degli interessati.

Purtroppo, però, come si è evinto anche dall'applicazione delle norme alle iscrizioni online al CRUA, rimangono ancora troppe lacune e i riferimenti che vengono forniti a titolari e responsabili dallo stesso Regolamento sono eccessivamente generici perché si possa garantire di aver gestito i dati degli utenti in modo davvero sicuro. È ovvio che non sarà mai possibile azzerare completamente i rischi a causa della natura stessa della Rete, ma è ancora lunga la strada per combattere ad armi pari le numerosissime minacce di divulgazione non autorizzata che ogni giorno incombono sui dati di ognuno di noi.

Per quanto riguarda i probabili sviluppi futuri applicabili al *web-form* CRUA, si può citare l'abilitazione del pagamento *online* (es. tramite *PayPal*, già predisposto ma non attivo), come alternativa al bonifico bancario per i non dipendenti dell'Università Politecnica delle Marche. L'attivazione di questa tipologia di pagamento implicherebbe la creazione di una connessione protetta per la comunicazione con il portale di PayPal (https://www.paypal.com/it/home), per garantire la sicurezza dell'utente che immette i suoi dati per il pagamento diretto sulla piattaforma.

Un'altra implementazione, seppur applicabile con un impegnativo lavoro di sviluppo (in ambito del progetto e della programmazione informatica) e un esborso monetario rilevante (a causa della necessità di introdurre, ad esempio, validazioni di tipo biometrico), potrebbe essere quella di un sistema di autenticazione della firma dell'utente che si vuole iscrivere al portale CRUA, in modo da snellire o, possibilmente eliminare, l'invio di documenti via e-mail successivamente all'inserimento dei dati.

# APPENDICE

Di seguito si riporta l'elenco dei file *php* compilati dalla sottoscritta (che costituiscono il *web-form* CRUA) e la rappresentazione dei loro collegamenti logici in due schemi riassuntivi, per *front-end* e *back-end*.

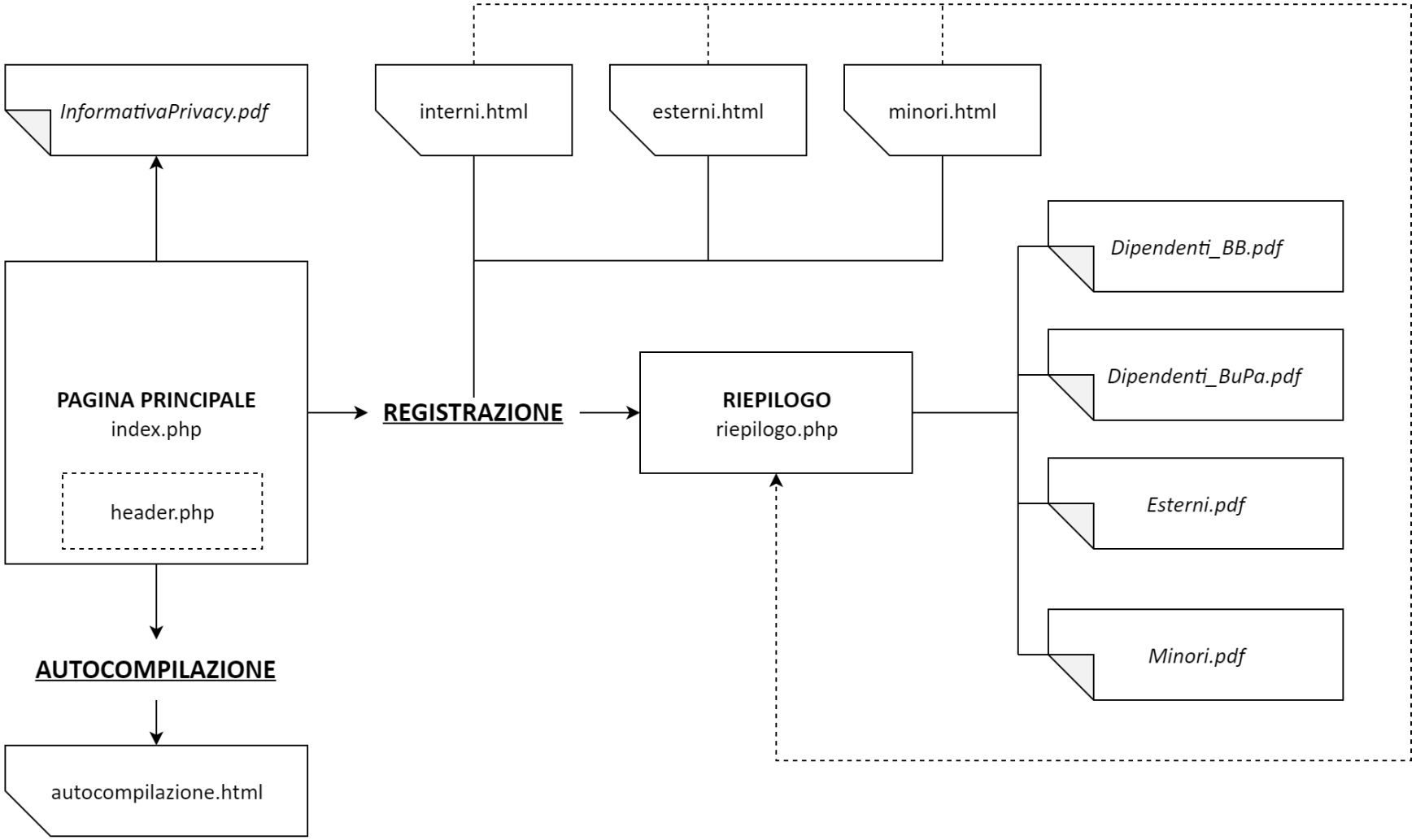
*FRONT-END*

I. *index.php*, nella directory "webformcrua" (417 righe di codice)
II. *riepilogo.php* nella directory "webformcrua" (340 righe di codice)
III. *registrazione.php*, nella directory "webformcrua" (251 righe di codice)
IV. *header.php*, nella directory "webformcrua/libs" (238 righe di codice)

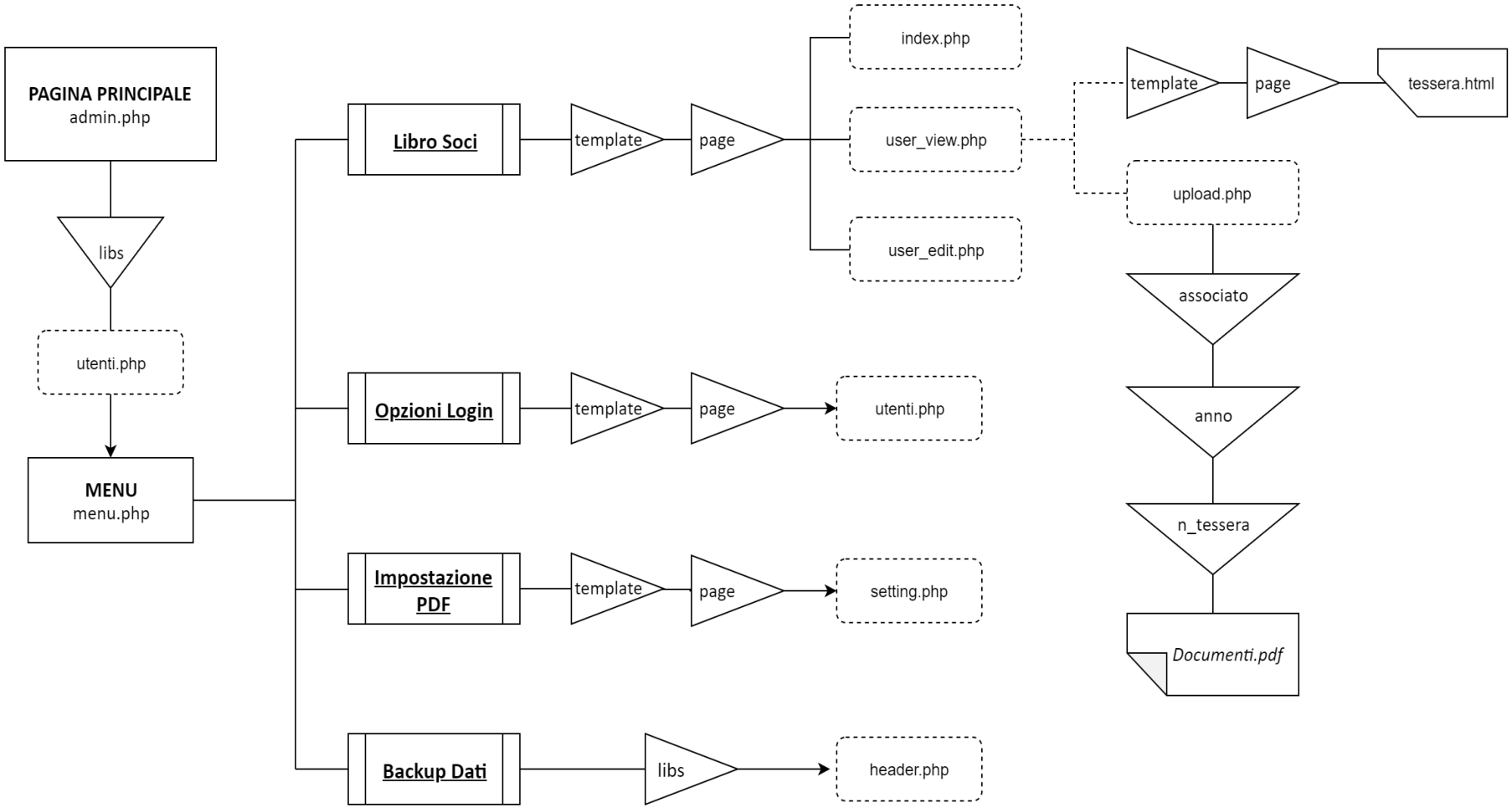
*BACK-END*

V. *login.php*, nella *directory* "webformcrua/template/page" (138 righe di codice)
VI. *admin.php*, nella *directory* "webformcrua/libs" (550 righe di codice)
VII. *index.php*, nella *directory* "webformcrua/template/page" (202 righe di codice)
VIII. *menu.php*, nella *directory* "webformcrua/template/page" (13 righe di codice)
IX. *upload.php*, nella *directory* "webformcrua/template/page" (105 righe di codice)
X. *iscrizione_edit.php*, nella *directory* "webformcrua/template/ page" (172 righe di codice)
XI. *user_edit.php*, nella *directory* "webformcrua/template/page" (105 righe di codice)
XII. *user_view.php*, nella *directory* "webformcrua/template/page" (391 righe di codice)
XIII. *setting.php*, nella *directory* "webformcrua/template/page" (73 righe di codice)
XIV. *utenti.php*, nella *directory* "webformcrua/template/page" (135 righe di codice)

# FRONT-END - Webform (struttura logica)



# BACK-END - Webform (struttura logica)



Di seguito sono riportate le funzioni che svolgono le azioni più significative per il funzionamento del *web-form*.

## FRONT-END (FE)

1. Controllo *check-box* "Interesse= Nessuno" – [*index.php*][I]

```
$("#InteresseNull").change(function(){
    if( $(this).is(":checked")){
        $("input[name='interesse[]'][value!='-1']").prop('checked',false).attr('disabled',true);
    }else{
        $("input[name='interesse[]'][value!='-1']").attr('disabled',false);
    }
});
```

Questa funzione permette di disabilitare (e bloccare) la selezione di tutte le altre caselle se la casella "Nessuno (esclude tutte le opzioni)" che ha valore -1 viene selezionata; finché quella casella non viene selezionata, è possibile selezionare tutte le altre.

2. Controllo sull'età inserita dall'utente – [*registrazione.php*][III]

```
if( $_POST["TipoSocioScelta"] == 1 || $_POST["TipoSocioScelta"] == 2 ){
    $testo = file_get_contents(__DIR__.DIRECTORY_SEPARATOR."template".DIRECTORY_SEPARATOR."email".DIRECTORY_SEPARATOR."interni.html");
}else{
    if( (date("Y-m-d")-$_POST["birth"]) < 14 )
        $testo = file_get_contents(__DIR__.DIRECTORY_SEPARATOR."template".DIRECTORY_SEPARATOR."email".DIRECTORY_SEPARATOR."minori.html");
    else
        $testo = file_get_contents(__DIR__.DIRECTORY_SEPARATOR."template".DIRECTORY_SEPARATOR."email".DIRECTORY_SEPARATOR."esterni.html");
}
```

Questa condizione analizza la tipologia dell'iscritto e, se non rientra nelle categorie "PTA" e "Docente", allora calcola la differenza tra la data del giorno in cui è effettuata l'iscrizione e la data di nascita inserita dall'utente: se il risultato è minore di 14 (anni) allora viene inviata l'*e-mail* apposita per i minorenni.

3. Data, ora e *IP* del *flag* relativo al consenso – [*registrazione.php*][III]

```
$queryInsertA = "INSERT INTO associato_anno (idAssociato,anno,tipoIscrizione,tipoSocio,interesse,privacy,address,city,pro,cap,tipoPagamento,service) VALUES (:associato,:anno,:tipoIscrizione,:tipoSocio,:interesse,'yes,".date("Y-m-d H:i:s").",".$ip."', :m_address,:m_city,:m_pro,:m_cap,:m_pag,:m_service)";
```

Questa *query* inserisce all'interno del *database* l'iscrizione annuale del socio e tra le colonne della tabella "associato_anno" vengono inseriti anche la data, l'orario e l'indirizzo *IP* dell'iscritto che presta il consenso.

4. Funzione per l'autocompilazione – [*index.php*][I]

```
$("#recovery").validate({
    rules: {
        emailTesseratoRecovery: {
            required: true,
            email : true
        }
    },
    errorElement: "em",
    errorPlacement: function (error, element) {
        error.addClass("help-block");
        element.addClass("has-feedback");
    },
    success: function (label, element) {
        if (!$(element).next("span")[ 0 ]) {
            $("<span class='glyphicon glyphicon-ok form-control-feedback'></span>").insertAfter($(element));
        }
    },
    highlight: function (element, errorClass, validClass) {
        $(element).addClass("is-invalid").removeClass("is-valid");
        $(element).next("span").addClass("glyphicon-remove").removeClass("glyphicon-ok");
    },
    unhighlight: function (element, errorClass, validClass) {
        $(element).addClass("is-valid").removeClass("is-invalid");
        $(element).next("span").addClass("glyphicon-ok").removeClass("glyphicon-remove");
    }, submitHandler: function (form) {
        $(form).find("button[type='submit']").attr('disabled',true);
        $.post("index.php", $(form).serialize(), function (d) {
            if (d.error != "" && d.message == null) {
                alert(d.error);
            } else {
                alert(d.message);
            }
            $(form).find("button[type='submit']").attr('disabled',false);
        }, "json");
        return false;
    }
});
```

Alla pagina *index.php*, dalla stessa pagina *index.php* viene inviata una richiesta del dato "codice fiscale" tramite comunicazione asincrona (fintanto che viene visualizzata la pagina all'utente viene inviata una richiesta alla pagina stessa). Dopo l'elaborazione della richiesta viene inviata un'*e-mail* dove è segnalato all'utente un *link* temporaneo per accedere nuovamente alla pagina *index.php* che stavolta sarà parzialmente compilata.

5. Obbligatorietà check-box consenso – [*index.php*][I]
   La funzione controlla la validità dei campi, secondo i criteri definiti all'interno di "rules" e se tutti i campi sono compilati correttamente, la funzione javascript nella pagina *index.php* invia una richiesta alla pagina *registrazione.php* che, a sua volta, controlla e valida i campi e inserisce la nuova iscrizione e invia un'*e-mail* all'iscritto.

## BACK-END (BE)

1. *Backup* dati (download file) – [*admin.php*][VI]
   Tramite la programmazione lato *server*, viene calcolata la grandezza del *file di backup* e ne viene validata la tipologia. Il *buffer* ottenuto (zona di memoria usata per compensare differenze di velocità nel trasferimento o nella trasmissione di dati, oppure per velocizzare l'esecuzione di alcune operazioni) viene inviato al *browser* (programma usato per visualizzare i siti *web* e per interagire con essi) che poi permette all'amministratore di scaricare il *file*.

2. Credenziali amministratori – [*utenti.php*][XIV]

   Per limitare l'accesso al *back-end* alle sole persone autorizzate, sono state introdotte delle credenziali (*username* e *password*) ed è possibile inserirne di nuove, modificarle o eliminarle.

3. *Download file pdf* – [*admin.php*][VI]
   Quando l'amministratore inoltra la richiesta di *download* del *file* dell'associato, il sistema ne controlla l'esistenza, la dimensione e la tipologia: il *buffer* ottenuto viene inviato al browser che poi permette di scaricare quel file. Simultaneamente il sistema salva, all'interno del *database*, una nuova riga contenente le informazioni relative all'amministratore che ha avuto accesso a quel *file*.

```php
if($pagina == "downloadFile"){
    $file = str_replace("../","",$_GET["f"]);
    if( empty($file) ){
        echo "Errore...";
    }else{
        if ($fd = fopen($file, "r")) {
            $fsize = filesize($file);
            $path_parts = pathinfo($file);
            $ext = strtolower($path_parts["extension"]);

            header("Content-type: application/octet-stream");
            header("Content-Disposition: filename=\"".$path_parts["basename"]."\"");
            header("Content-length: $fsize");
            header("Cache-control: private"); //use this to open files directly

            $user = $myPDO->prepare("INSERT INTO access_list ( idUser,dataEvento,ipEvento,FileDownload ) "
                    ." VALUES ( :utente, :dEvento, :RemoteAddress, :file )");
            $user->bindParam(":utente", $_SESSION["auth_id"], PDO::PARAM_STR);
            $user->bindParam(":dEvento", date("Y-m-d H:i:s"), PDO::PARAM_STR);
            $user->bindParam(":RemoteAddress", $ip, PDO::PARAM_STR);
            $user->bindParam(":file", $file, PDO::PARAM_STR);
            $user->execute();

            while (!feof($fd)) {
                $buffer = fread($fd, 2048);
                echo $buffer;
            }
        }
        fclose($fd);
    }
    exit;
}
```

4. <u>Eliminazione utente</u> – [*admin.php*][VI]

```php
if ($pagina == "user_delete") {
    if (!is_numeric($_GET["id"])) {
        header("Location: admin.php");
    } else {
        $user = $myPDO->prepare("SELECT * FROM associato WHERE id = :c");
        $user->bindParam(":c", $_GET["id"], PDO::PARAM_STR);
        $user->execute();
        $utenti = $user->fetch(PDO::FETCH_ASSOC);

        if (!$utenti) {
            header("Location: admin.php");
        } else {
            $user = $myPDO->prepare("DELETE FROM associato WHERE id = :c");
            $user->bindParam(":c", $_GET["id"], PDO::PARAM_STR);
            $user->execute();

            $user = $myPDO->prepare("DELETE FROM associato_anno WHERE idAssociato = :c");
            $user->bindParam(":c", $_GET["id"], PDO::PARAM_STR);
            $user->execute();
            header("Location: admin.php");
        }
    }
}
```

Questa funzione permette l'eliminazione completa dei dati relativi all'iscritto (senza però eliminare gli eventuali *file pdf* associati).

5. Esportazione dell'elenco associati in file xls – [*admin.php*][VI]
   Questa funzione permette di esportare tutto l'elenco soci all'interno di un *file* in formato xls. Vengono richiesti al *database* tutti i dati degli iscritti all'anno indicato e, una volta ricevuti, vengono analizzati e incolonnati e viene inviato un *buffer* al *browser* che così ne permette il *download*.

6. Modifica scheda associato – [*user_edit.php*][XI]
   I nuovi dati inseriti dall'amministratore aggiornano il *database*. È possibile modificare sia i dati relativi all'anagrafica generale dell'associato o del singolo anno di tesseramento.

7. *Password PDF* – [*upload.php*][IX]

```php
try{
    $writer = new setasign\FpdiProtection\FpdiProtection();
    $ownerPassword = $writer->setProtection(
            setasign\FpdiProtection\FpdiProtection::PERM_PRINT | setasign\FpdiProtection\FpdiProtection::PERM_DIGITAL_PRINT |
            setasign\FpdiProtection\FpdiProtection::PERM_MODIFY,
            $passwordSet, //user password per visualizzazione/stampa
            $passwordSet, //password proprietario per l'eventuale modifica del pdf
            3
    );

    $pageCount = $writer->setSourceFile($fileCrypt);
    for ($pageNo = 1; $pageNo <= $pageCount; $pageNo++) {
        $id = $writer->importPage($pageNo);
        $size = $writer->getTemplateSize($id);
        $writer->AddPage($size['orientation'], $size);
        $writer->useTemplate($id);
    }
    $writer->Output('F', str_replace($result["name"],$result["name"],$fileCrypt ),true);
}catch(Exception $a){
    echo $a->getMessage();
}
```

Nella pagina *upload.php* è stato inserito un metodo per impostare una *password* ai documenti (in formato *pdf*) caricati dagli amministratori. Una volta ricevuto il *file* dalla funzione *upload*, il sistema imposta automaticamente la *password* che gli amministratori hanno settato in precedenza.

8. *Upload PDF* – [*upload.php*][IX]

   L'*uplad* funziona sul lato client e sul lato *server*. Sul lato *client* viene gestito da una funzione *javascript* che invia, con comunicazione asincrona, piccoli pacchetti del file alla pagina *upload.php*. Sul lato server la pagina *upload.php* salva i pacchetti ricevuti e, al momento della ricezione dell'ultimo, unisce i singoli pacchetti e salva sul *server* il file ottenuto dall'unione.

# FONTI BIBLIOGRAFICHE E SITOGRAFIA

Anche se non specificato, tutte le informazioni tecnico/giuridiche sono tratte direttamente dal "Regolamento Generale sulla Protezione dei Dati" - "GDPR: General Data Protection Regulation" – "Regolamento UE 679/2016" [1] e da guide ufficiali per la sua interpretazione [5, 13, 14, 15].


1. *Testo ufficiale del GDPR* (ultimo accesso 04/12/2019): https://www.privacyitalia.eu/wp-content/uploads/2017/10/GDPR_Italiano_PDF.pdf

2. Associazione Culturale, *GDPR: Nuove normative sulla Privacy UE* (ultimo aggiornamento 20/06/2018): http://associazione-culturale.it/gdpr-privacy-e-trattamento-dati/
3. Bianchi M., *GDPR: Cosa Cambia Con Il Nuovo Regolamento Privacy Europeo? Dal D. Lgs 196/2003 Al Reg. 2016/679/UE* (ultima modifica 25 gennaio 2018): https://www.cyberlaws.it/2018/gdpr-differenze-2016-679-ue-dlgs-196-2003/
4. Calò A.L., *GDPR: il nuovo Regolamento europeo (2016/679) per la social privacy* (ultimo accesso 05/12/2019): www.lifelearning.it
5. Celella R., *Guida alla lettura del decreto 101/2018 di adeguamento della normativa nazionale al GDPR* (ultimo accesso 05/12/19): https://www.dataprotectionlaw.it/decreto-101-2018-di-adeguamento-della-normativa-nazionale-al-gdpr/
6. Cookie Law GDPR, *What is Opt-in and Opt-out in GDPR?* (ultima modifica 3 settembre 2019): https://www.cookielawinfo.com/what-is-opt-in-and-opt-out-in-gdpr/
7. De Stefani F., *Le regole della privacy*: *Guida pratica al nuovo GDPR,* Milano: Editore Ulrico Hoepli, 2018

8. InfoGDPR, *Il GDPR e il trattamento di dati personali* (ultimo aggiornamento 09/02/2018): https://www.infogdpr.eu/trattamento-dati-personali-gdpr-13.html
9. InfoGDPR, *Pseudonimizzazione: che cos'è e cosa viene richiesto dal GDPR* (ultimo aggiornamento 10/02/2018): https://www.infogdpr.eu/pseudonimizzazione-gdpr-58.html
10. Filippi C., *Regolamento UE. Il Garante privacy incontra la P.A. (Bari, 15/01/18) - 5) ADEMPIMENTI* – Garante *Privacy*: https://www.youtube.com/watch?v=KtR1lqVkzb8
11. Garante Privacy, *Cosa intendiamo per dati personali?* (ultimo accesso 04/12/2019): https://www.garanteprivacy.it/web/guest/home/diritti/cosa-intendiamo-per-dati-personali
12. Garante Privacy, *Diritti degli interessati* (ultimo accesso 04/12/2019): https://www.garanteprivacy.it/web/guest/regolamentoue/diritti-degli-interessati
13. Garante Privacy, *Guida all'applicazione del Regolamento Europeo 2016/679 in materia di protezione dei dati personali* (edizione aggiornata a febbraio 2018): https://www.garanteprivacy.it/documents/10160/0/Guida+all+applicazione+del+Regolamento+UE+2016+679.pdf/2281f960-a7b2-4c53-a3f1-ad7578f8761d?version=1.3
14. Garante *Privacy*, *Regolamento UE 2016 679. Arricchito con riferimenti ai Considerando Aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018* (ultimo accesso 04/12/2019): https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Considerando+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale+

+dell%27Unione+europea+127+del+23+maggio+2018.pdf/1bd9bde0-d074-4ca8-b37d-82a3478fd5d3?version=1.9

15. Gazzetta Ufficiale, *Decreto Legislativo 10 agosto 2018, n. 101* (ultimo accesso 04/12/19): http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=true
16. Garante *Privacy, Individuazione e gestione del rischio, Tutorial, slide* (ultimo accesso 04/12/2019): https://www.garanteprivacy.it/documents/10160/0/Individuazione+e+gestione+del+rischio+-+Tutorial+-+slide.pdf/d2eb9375-c577-4ff3-b716-38cc703ec26f?version=1.0
17. Gradozzi F., Leonarduzzi S., Libertini G., *Privacy in regola: Comprendere il Regolamento UE 2016/679 sulla protezione dei dati personali ("GDPR") e orientarsi nell'adeguamento ai nuovi obblighi [Seconda edizione aggiornata al D. Lgs. 8 Agosto 2018, n.101 e ampliata con il modulo sull'analisi e la gestione del rischio "privacy"],* Polonia: Amazon Fullfillment, 2019
18. Iso.org, *ISO 31000 Risk Management* (ultimo accesso 04/12/2019): https://www.iso.org/iso-31000-risk-management.html
19. Manuelli R., *Principio di accountability* – GDPR scuola (ultimo accesso 04/12/2019): https://gdprscuola.it/il-principio-di-accountability/
20. Pennasilico A., *GDPR: l'analisi del rischio* (ultima modifica 08/01/2018): https://www.zerounoweb.it/techtarget/searchsecurity/gdpr-lanalisi-del-rischio/
21. PrivacyLab, *I dati sensibili nel GDPR* (ultimo aggiornamento 06/12/2019): https://www.privacylab.it/IT/205/I-dati-sensibili-nel-GDPR/

22. Saetta B., *Privacy by design e by default* - Protezione Dati Personali (25/03/2018): https://protezionedatipersonali.it/privacy-by-design-e-by-default
23. Saetta B., *Valutazione di impatto (DPIA) e rischio del trattamento* (ultima modifica 16 settembre 2019): https://protezionedatipersonali.it/valutazione-impatto-e-rischio-trattamento
24. Viggiano M., *Regolamento UE. Il Garante privacy incontra la P.A. (Bari, 15/01/18) - 8) DPIA* – Garante *Privacy*: https://www.youtube.com/watch?v=3pIwx2I6iIc
25. Wikipedia, Drupal (ultimo accesso 04/12/2019): https://it.wikipedia.org/wiki/Drupal
26. Wikipedia, Iframe (ultimo accesso 04/12/2019): https://it.wikipedia.org/wiki/Iframe

27. Iscrizione a Circolo UniPG: http://www.circolosanmartino.unipg.it/documenti/iscrizioni
28. Iscrizione a CRAL Basilicata: http://cral.regione.basilicata.it/iscrizione/
29. Iscrizione online su Portal Arci: https://portale.arci.it/preadesione/circolo-ricreativo-campo/
30. Registrazione online sull'ACI (Automobile Club Italia): https://login.aci.it/index.php?do=genNotAuth&id=register&application_key=aruisa
31. Registrazione su Eventbrite (sito di eventi): https://www.eventbrite.it/l/registrazione-online/
32. Registrazione online su Il Portale dell'Automobilista: https://www.ilportaledellautomobilista.it/web/portale-automobilista/certifica-mail-cittadino
33. Registrazione online su Job Italia (Agenzia per il Lavoro):

https://firmadigitale.jobitalia.net/JobItalia/view.candidato.registrazione.do

34. Registrazione online su LaFeltrinelli (catena di librerie): https://www.lafeltrinelli.it/fcom/it/home/login.html
35. Registrazione online su sito Mondadori (catena di librerie): https://www.hubscuola.it/utente-registrazione
36. Registrazione online Nintendo (azienda *leader* nel campo videoludico): https://accounts.nintendo.com/authorize_age_gate
37. Registrazione online su Poste Italiane: https://www.poste.it/registrazione/registrazione.html#/
38. Registrazione online su Randstad (Agenzia per il Lavoro): https://extranet.randstad.it/Candidato/Registrazione/Comincia-da-qui
39. Registrazione online sulla SIAE (Società Italiana degli Autori ed Editori): https://www.siae.it/it/servizi-online
40. Registrazione online su Umana (Agenzia per il Lavoro): https://areacandidato.umana.it/area-candidato/iscrizione
41. Registrazione online su Unieuro (catena di negozi di elettronica): https://www.unieuro.it/online/register

# NOTE

Il *web-form* a cui ci si riferisce in questa tesi è stato realizzato dalla sottoscritta, sotto la supervisione del Prof. Primo Zingaretti ed è un progetto didattico sperimentale atto a "prestare forma" a quanto asserito in questo testo.

Non sono mai stati inseriti dalla sottoscritta dati relativi a persone realmente esistenti e/o iscritte realmente al C.R.U.A., pertanto la sottoscritta non è indicabile né come titolare al trattamento dati, né come responsabile dei dati, né come referente alcuno per i dati trattati dal Circolo Ricreativo Universitario di Ancona (C.R.U.A.) e dagli eventuali individui (o associazioni) delegati.

Inoltre, tutti i documenti in *pdf* accessibili dagli utenti e inviati ad essi (in particolare l'Informativa sulla *Privacy* a cui si accede tramite il *web-form*, attraverso il clic su "Selezionando la casella e cliccando sul tasto "Registrati", DICHIARO di aver letto e accettato le condizioni descritte nell'Informativa sulla *Privacy* (clicca qui per accedere all'informativa)"), NON sono stati né formulati né redatti dalla sottoscritta. Pertanto, declino ogni responsabilità relativa all'eventuale non idoneità degli stessi.

Spetta infatti al titolare e al responsabile del trattamento dati verificare che le misure di sicurezza adottate e la gestione dei dati relativi al Circolo Ricreativo Universitario di Ancona siano idonee e conformi alle norme del Regolamento UE 679/2016 (Regolamento Generale della Protezione dei Dati - GDPR).