Designazione a "Persona autorizzata al trattamento dei dati personali" ai sensi del Regolamento UE n.679/2016 (GDPR), del D.lgs. n.196/2003 (Codice Privacy) e del D.lgs. n.101/2018

Con la presente **Roberto Enrico Barbieri** in qualità di Direttore Generale e quindi Titolare del Trattamento Dati di Oxfam Italia, la designa come **persona autorizzata al trattamento dei dati personali ai sensi del Regolamento UE n.679/2016 (GDPR), del D.lgs. n.196/2003 (Codice Privacy) e del D.lgs. n.101/2018**
Attraverso la seguente nomina dovrà attenersi, nello svolgimento della sua attività, a quanto riportato nelle seguenti **Istruzioni per il trattamento dei dati personali** per la **corretta gestione all'interno di tutte le attività definite per la sua collaborazione.**

La modalità di gestione del trattamento dei dati è basata sui Principi Generali definiti dal Regolamento Europeo 679/2016 GDPR *e* D. Lgs. 2018/101 e sulla base degli stessi, **gli autorizzati al trattamento dei dati personali devono scrupolosamente attenersi alle seguenti istruzioni che devono essere considerate ordine di servizio**.

I dati personali devono essere conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e trattati e comunque nel rispetto di quanto definito nel **registro del trattamento dei dati personali.**

Per tutte le regole relative all'utilizzo della strumentazione informatica e della rete intranet, si rimanda al **Regolamento Informatico**[2]

Al fine di garantire l'utilizzo dell'intelligenza artificiale in maniera conforme al Regolamento UE 679/2016 e D. Lgs. 2018/101 si rimanda alle **Linee Guida AI Generativa**[3]

1. **Obbligo di riservatezza nel trattamento dei dati personali e delle informazioni di Oxfam Italia**

In riferimento alla designazione come "Persona autorizzata al trattamento dei dati personali" ai sensi del Regolamento UE n.679/2016 (GDPR), del D.lgs. n.196/2003 (Codice Privacy) e del D.lgs. n.101/2018 e alle istruzioni per il trattamento dei dati, la persona autorizzata al trattamento dei dati personali si obbliga:

1. a trattare i dati personali unicamente in base alle istruzioni ricevute dall'Organizzazione e, in ogni caso, in conformità con la normativa vigente in materia di protezione dei dati personali;
2. a garantire che i dati personali siano trattati nel rispetto dei principi e delle norme applicabili di legge e in stretta osservanza alle istruzioni fornitemi. In particolare, si impegna a che i dati personali oggetto di trattamento nello svolgimento delle mansioni lavorative siano:

- trattati solo se necessario e solo nella misura necessaria al raggiungimento delle legittime finalità del trattamento ("minimizzazione dei dati");
- sempre corretti e, se necessario, aggiornati;
- conservati in modo tale da consentire l'identificazione degli interessati solo per il periodo di tempo necessario al raggiungimento delle finalità per le quali vengono trattati;
- trattati in modo tale da assicurare un adeguato livello di sicurezza, ivi inclusa la tutela da accessi o trattamenti non autorizzati o illeciti e da perdita accidentale, distruzione o danneggiamento, ricorrendo ad idonee misure tecniche ed organizzative ("integrità e riservatezza").

3. osservare la più stretta riservatezza con riferimento ai dati personali e informazioni raccolte e trattate, o ai quali avrà accesso nell'ambito dell'attività svolta per l'Organizzazione e a non farne o tenerne copia, a non rivelarli ad alcuna altra persona fisica o giuridica, ivi inclusi altri membri del personale, che non siano espressamente autorizzati all'accesso per istruzione dell'Organizzazione, contratto o legge.

L'obbligo di non divulgazione e riservatezza è a tempo indeterminato e resta fermo anche qualora dovesse cessare il rapporto con l'Organizzazione.

La persona autorizzata al trattamento dei dati è consapevole che:
1. che qualsiasi violazione dell'obbligo di riservatezza o, in generale, delle norme di legge poste a tutela dei dati personali può comportare, nei confronti dell'Organizzazione, l'imposizione di rilevanti sanzioni ai sensi delle disposizioni di cui al Codice Privacy e ai sensi delle disposizioni di cui al GDPR e delle altre

disposizioni applicabili in materia, nonché causare danni a persone fisiche o giuridiche, ivi inclusa l'Organizzazione;
2. della natura vincolante delle istruzioni di trattamento fornitemi dall'Organizzazione e che la trasgressione a tali istruzioni, e alle norme contenute nel presente accordo, può comportare l'irrogazione di sanzioni disciplinari previste dal contratto di lavoro e dalla normativa applicabile (ivi incluse penali qualora previste), oltre al risarcimento del danno eventualmente arrecato in esito alle violazioni perpetrate.

2. Informativa e raccolta dei dati personali per conto di Oxfam Italia

I dati personali, comprese le immagini e video, dovranno essere raccolti utilizzando apposite **schede di raccolta dati,** validate dal Quality & Compliance Office e assicurandosi che alle persone interessate venga sempre resa l'informativa.
L'informativa completa è allegata alle schede di raccolta dati, disponibile sul sito Privacy Policy - Oxfam Italia e **stampabile**

Per i dati riguardanti i minori sotto i 18 anni sarà necessario sempre il consenso da parte di chi esercita la potestà genitoriale.
I dati raccolti dovranno pervenire al CRM Manager utilizzando il **tracciato anagrafiche** e non potranno esser diffusi o conservati in archivi esterni alle sedi dell'Organizzazione.
Qualora si rendano necessarie modifiche o integrazioni alle schede o al testo dell'informativa dovrà essere inviata una richiesta a privacy@oxfam.it

In caso di problemi di accesso al link scrivere a itc@oxfam.it

3. **Archivio e gestione dei documenti**

Tutta la documentazione generata per la raccolta dei dati personali, sia in modalità cartacea che informatica dovrà rimanere in giacenza per il solo tempo necessario allo svolgimento delle sue funzioni o fino a revoca specifica dell'interessato.
Tutti i documenti cartacei dovranno essere gestiti in modo da ridurre al minimo i tempi di permanenza fuori degli archivi o degli armadi o contenitori presenti nelle sedi organizzative.
Tutta la documentazione cartacea generata e/o prodotta al di fuori delle sedi organizzative, prestando particolare attenzione, dovrà essere consegnata al proprio Referente. Successivamente dovrà essere conservata all'interno dell'Organizzazione in spazi che ne garantiscano la riservatezza.

Massima attenzione dovrà essere posta per i documenti che si trovano in locali condivisi e accessibili al pubblico; chi provvede alla duplicazione di documenti con stampanti, macchine fotocopiatrici o scanner, in caso di copia erronea o non leggibile correttamente, da cui potrebbero essere desunti dati personali, è tenuto a distruggere il documento in modo da escludere qualunque possibilità da parte di estranei di venire a conoscenza dei dati medesimi e non ad utilizzare il documento come carta da riciclo.
I documenti contenenti dati personali devono essere immediatamente presi dalla persona che ha provveduto alla stampa o duplicazione.

Quando si effettuano scansioni si raccomanda di eliminare i documenti dalla cartella dello scanner una volta trasferiti i file sul proprio computer.

L'accesso agli archivi è consentito solo al personale espressamente autorizzato in via permanente o occasionale.

Nelle attività in cui possono essere trattati dati particolari o giudiziari dovrà essere posta la massima attenzione a limitare al minimo indispensabile la giacenza della documentazione al di fuori degli armadi o contenitori muniti di serratura; controllare con particolare rigore l'accesso ai propri archivi; segnalare alla segreteria eventuali accessi negli uffici compiuti al di fuori degli usuali orari di apertura/chiusura.

Gli archivi dovranno essere mantenuti costantemente chiusi, compatibilmente con le esigenze di servizio.
Le copie dei documenti vanno trattate, con riferimento alla tutela dei dati personali in esse contenuti, con la medesima diligenza riservata agli originali.

4. **Attivazione e utilizzo dei Siti Web e Social di proprietà di Oxfam Italia**

Qualora per i progetti o attività gestiti vi sia la necessita di attivare e/o gestire siti WEB e/o pagine Social che utilizzano il logo di Oxfam Italia è obbligatorio ricevere l'autorizzazione all'utilizzo del logo dalla Head of Brand & Mass Marketing Unit.

A seguito del nulla osta si dovrà fare riferimento all'Information System & Facility Office scrivendo a itc@oxfam.it e al Quality & Compliance Office scrivendo a privacy@oxfam.it per garantire tutte le disposizioni relative alla privacy e per la scelta del fornitore.

5. Nomina Responsabili Esterni del Trattamento dei dati personali

Tutti i fornitori che trattano i dati personali per conto di Oxfam Italia dovranno ricevere un **Incarico scritto come Responsabile esterno al Trattamento dei dati personali**[4]**.**

Tale modello dovrà essere integrato con:

- Descrizione delle categorie di dati personali trattati dal fornitore per conto di Oxfam Italia;
- Istruzioni da parte di Oxfam Italia al fornitore sulle garanzie e tutele da attuare per la gestione dei dati personali;
- Indicazioni sulle modalità di trasmissione dei dati personali in maniera protetta.

L'incarico come Responsabile Esterno al trattamento dei dati personali potrà essere rivisto, se richiesto, dal Quality & Compliance Office scrivendo a privacy@oxfam.it

Nel caso di trasferimento di dati personali a Enti incaricati come Responsabili Esterni del Trattamento, le modalità di trasmissione sicura dei dati dovranno essere definite all'occorrenza scrivendo a itc@oxfam.it

6. Ulteriori adempimenti per il Personale che svolge attività in locali esterni alle sedi organizzative

Per lo svolgimento di attività in locali esterni alle sedi organizzative dovrà essere resa la massima attenzione alla protezione dei dati personali e garantire che venga adottato in qualsiasi occasione e contesto un comportamento improntato alla sicurezza dei dati personali degli interessati, in linea con il ruolo che viene svolto nel sistema privacy aziendale e in ottemperanza al principio di accountability (responsabilizzazione).

Il luogo di lavoro potrà essere individuato nel proprio domicilio o altro luogo privato purché presenti caratteristiche ambientali che garantiscano riservatezza, un ambiente protetto, silenzioso e dotato di adeguati sistemi che consentano la connettività sicura, evitando l'utilizzo di WI-FI a reti aperte.

È vietato svolgere la prestazione lavorativa in locali pubblici o aperti al pubblico che possano mettere a rischio la sicurezza fisica del personale lavorativo stesso e la sicurezza dei dati aziendali.

Qualsiasi conversazione di lavoro non dovrà essere oggetto di ascolto da parte di altri soggetti non autorizzati, i quali devono essere mantenuti ad una distanza che consenta di proteggere la confidenzialità e la riservatezza; è pertanto obbligatorio:

- Non effettuare colloqui ad alta voce, di persona o per telefono, in presenza di soggetti non autorizzati a conoscere il contenuto della conversazione;
- Nel caso di conversazioni telefoniche instaurate in seguito di chiamate inoltrate o ricevute, dovrà essere accertato che l'interlocutore sia effettivamente legittimato e autorizzato a conoscere le informazioni oggetto della comunicazione.

7. Norme di comportamento in caso di Data Breach

In caso di Data Breach (violazione dei dati personali da parte di soggetti esterni all'organizzazione) dovrà essere segnalata immediatamente la circostanza scrivendo a itc@oxfam.it e a privacy@oxfam.it per consentire l'espletamento di tutti gli obblighi nei tempi previsti dalla legge.

Dovranno contestualmente essere fornire le seguenti informazioni:

- natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati;
- probabili conseguenze della violazione dei dati personali;
- eventuali misure adottate nell'immediatezza dell'evento o che si possono adottare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
- riferimenti telefonici per essere contattabile per ogni ulteriore approfondimento e richiesta di informazioni.

Si sottolinea l'importanza della tempestività nel segnalare il Data Breach e nel fornire tutte le informazioni richieste, per consentire al Titolare di effettuare la segnalazione al Garante Privacy entro il termine di 72 ore dall'individuazione dell'incidente.

Per qualsiasi altra informazione o richiesta di autorizzazione in materia può inviare una mail a privacy@oxfam.it