SviluppoToscana S.p.A.

Regolamento per l'utilizzo dei sistemi informatici e telematici

di Sviluppo Toscana Sp.A. [1]

Firenze, 24 Ottobre 2019

[1] Il regolamento - ***redatto tenendo conto Disposizione dell'Amministratore Unico n. 40 del 01/10/2018 ha adottato le indicazioni operative per la formulazione di linee guida in materia di protezione dati personali (vedi allegato Disposizione dell'Amministratore Unico di Sviluppo Toscana S.p.A. n. 40 del 01 /10/2018 - Regolamento (UE) 2016/679 "Regolamento Generale sulla Protezione dei Dati" (GDPR) - Adozione delle indicazioni operative per la formulazione di linee guida in materia di protezione dati personali al fine di garantire la compliance dei trattamenti al GDPR.***

Indice

Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone *Sviluppo Toscana* e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, Sviluppo Toscana ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati. Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del Reg. (UE) 2016/679 "Regolamento generale sulla protezione dei dati" e della normativa nazionale.

Considerato inoltre che Sviluppo Toscana, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, telefoni cellulari, etc.), sono state inserite nel regolamento alcune clausole relative alle modalità ed i doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

1. Oggetto e finalità

Il presente Regolamento è redatto:

- alla luce della Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- in attuazione del Regolamento Europeo 679/16 "General Data Protection Regulation" (d'ora in avanti Reg. 679/16 o GDPR);
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- alla luce dell'articolo 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa».

La finalità è quella di promuovere in tutto il personale una corretta "cultura informatica" affinché l'utilizzo degli Strumenti informatici e telematici forniti dall'Ente sia conforme alle finalità per le quali sono state messe a disposizione del personale e nel pieno rispetto della legge. Si vuole fornire a tutto il personale le indicazioni necessarie con l'obiettivo principale di evitare il verificarsi di qualsiasi abuso o uso non conforme, muovendo dalla convinzione che la prevenzione dei problemi sia preferibile rispetto alla loro successiva correzione.

2. Entrata in vigore del regolamento e pubblicità

2.1 Il nuovo regolamento supera il precedente regolamento ed entrerà in vigore dal 24 Ottobre 2019

Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

2.2 Copia del regolamento verrà messa a disposizione di ciascun dipendente e collaboratore della società attraverso la rete Intranet.

3. Campo di applicazione del regolamento

3.1 Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).

4. Utilizzo del Personal Computer

4.1 **Il Personal Computer affidato all'utente è uno strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

4.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete di *Sviluppo Toscana* solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto 4 del presente Regolamento.

4.3 Sviluppo Toscana rende noto che il personale incaricato che opera presso il servizio Information and Communication Tecnology[2] (nel seguito per brevità "Servizio ICT") della stessa Sviluppo Toscana è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). Detti interventi, in considerazione dei divieti di cui ai successivi punti nn. 8.2 e 9.1, potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata od impedimento dell'utente.

L'accesso ai dati e al PC potrà essere effettuato da remoto. L'accesso dal PC da parte del personale incaricato viene segnalato da un apposita icona posta sulla barra delle applicazioni.

4.4 Il personale incaricato del servizio ICT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

4.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio ICT per conto della *Sviluppo Toscana* né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la stessa *Sviluppo Toscana* a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema di software regolarmente licenziato o comunque libero, vengono sanzionate anche penalmente. A tal fine Sviluppo Toscana ha installato un apposito software di monitoraggio delle applicazioni installate che consente fra l'altro l'installazione senza interazione con il PC di nuove applicazioni che si possano ritenere utili ai fini aziendali e la disinstallazione di applicazioni superflue o obsolete.

4.6 Salvo preventiva espressa autorizzazione del personale del Servizio ICT, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …).

---

[2] O altra figura aziendale preposta alla gestione del sistema informatico aziendale, indipendentemente da una sua nomina a Responsabile della privacy ai sensi dell'art. 29 del D.lgs. 196/2003. Nel caso la gestione del sistema ICT (o di alcune fasi di esso) siano affidate a terzi, saranno adottate idonee clausole contrattuali volte a formalizzare l'attribuzione delle relative responsabilità.

4.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio ICT nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.

4.8 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso[3]**.**

5. Gestione ed assegnazione delle credenziali di autenticazione

5.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio ICT, previa formale richiesta del Responsabile di ASA (o di Attività) nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

5.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal Servizio ICT, associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Servizio ICT.

5.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

5.4 È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi (Ogni tre mesi nel caso in cui l'incaricato invece tratti dati sensibili attraverso l'ausilio di strumenti elettronici).

5.5 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del Servizio ICT.

5.6 Soggetto preposto alla custodia delle credenziali di autenticazione è il personale incaricato del Servizio ICT di *Sviluppo Toscana.*[4]6. Utilizzo della rete di Sviluppo Toscana

6.1 Per l'accesso alla rete di *Sviluppo Toscana* ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

6.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parola chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

6.3 Le cartelle utenti presenti nei server di *Sviluppo Toscana* sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del personale del Servizio ICT. Si ricorda inoltre che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale incaricato del Servizio ICT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente. A tal fine per evitare data breach (art 33 e 34 regolamento GDPR) è assolutamente vietato archiviare dati aziendali, di cui non si abbia altra copia, sulle unità locali e/o su dischi rimovibili.

6.4 Il personale del Servizio ICT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

---

[3] Una modalità automatica che evita di lasciare incustodito il pc, anche in caso di mancato spegnimento da parte dell'utente è quello di adottare il savescreen a tempo con obbligo di reintrodurre la password per l'accesso.

[4] Solo per le caselle di posta elettronica certificata e le credenziali di utente privilegiato sui server

6.5 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

7. Utilizzo e conservazione dei supporti rimovibili

7.1 Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

7.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Servizio ICT e seguire le istruzioni da questo impartite.

7.3 In ogni caso, i supporti magnetici contenenti dati personali devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

7.4 E' vietato l'utilizzo di supporti rimovibili personali. E' obbligatorio fare uso di supporti aziendali restituendoli dopo l'uso al personale incaricato della custodia.

7.5 L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

7.6 In caso di trasporto di dati personali su chiavette USB aziendali è opportuno che i dati vengano memorizzati sulle chiavette in archivi protetti da password in modo da garantire che in caso di smarrimento i dati non siano facilmente accessibili a chi dovesse entrare in possesso del supporto.

7.7 In caso di smarrimento dei supporti, è necessario fare riferimento alle indicazioni del DPO relative allo smarrimento, furto, distruzione danneggiamento della strumentazione di lavoro allegato alla presente policy.

8. Utilizzo di PC portatili

8.1 L'utente è responsabile del PC portatile assegnatogli dal Servizio ICT e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

8.2 Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

8.3 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

8.4 Tali disposizioni si applicano anche nei confronti di incaricati esterni quali agenti, forza vendita, ecc.

8.5 Come per i supporti rimovibili in caso di smarrimento/furto/danneggiamento è necessario fare riferimento alle indicazioni del DPO relative allo smarrimento, furto, distruzione danneggiamento della strumentazione di lavoro allegato alla presente policy.

8.6 E' strettamente vietato l'uso di PC portatili/tablet personali in ambito aziendale. Qualora per cause di forza maggiore o indisponibilità degli strumenti aziendali, tale utilizzo si renda necessario al di fuori della sede di appartenenza, lo stesso deve essere preventivamente autorizzato dalla Direzione. In caso di smarrimento il dipendente dovrà darne immediata comunicazione all'azienda, come se si trattasse di strumentazione aziendale (ved. Punto 7.5).

8.7 Nel caso di utilizzo di PC portatili personali è comunque obbligatorio che l'accesso avvenga tramite password.

9. Uso della posta elettronica

9.1 **La casella di posta elettronica assegnata all'utente è uno strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

9.2 È fatto divieto di utilizzare le caselle di posta elettronica ***……..@sviluppo.toscana.it*** per motivi diversi da quelli strettamente legati all'attività lavorativa, si ricorda che tale casella è aziendale e non personale sebbene riporti il nome del lavoratore. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
-
- 9.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

9.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per *Sviluppo Toscana* ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Responsabile d'ufficio.

9.5 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

9.6 È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

9.7 Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere attivata dall'utente.

9.8 In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni - verrà attivata a cura dell'azienda.

9.9 Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dall'azienda, accedere, mediante cambio della password da parte del Servizio ICT, alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui al punto 8.7; assenza non programmata ed impossibilità di attendere i due giorni di cui al punto 8.8).

9.10 Il personale del servizio ICT, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 3.3[5].

9.11 Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy aziendale. Gli accessi degli utenti alle caselle di posta elettronica vengono tracciati e mantenuti in un log per la durata di 30gg.

10. Navigazione in Internet

10.1. **Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività**

[5] L'accesso ai contenuti della corrispondenza nella casella di posta elettronica avviene esclusivamente in caso di assenza prolungata od impedimento dell'utente secondo quanto prescritto dal punto 10 del disciplinare tecnico legato al codice mediante cambio della password dell'utente per lendere palese allo stesso l'avvenuto accesso.

lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

10.2 In questo senso, a titolo puramente esemplificativo, **l'utente non potrà utilizzare internet** per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del Servizio ICT);
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dall'Amministratore Unico (o eventualmente dal Responsabile di ASA e/o del Servizio ICT) e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali e comunque non autorizzati preventivamente dalla direzione aziendale, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio.

L' accesso, tramite internet, a caselle webmail di posta elettronica personale è consentito solo durante l'orario di pausa pranzo ed esclusivamente solo da dispositivi personali. Qualora i detti dispositivi siano stati autorizzati anche per un utilizzo aziendale, l'utente dovrà comunque porre la massima attenzione nell'aprire i file allegati ai messaggi di posta elettronica prima del loro utilizzo.

La possibilità di accedere a Facebook e agli altri social network, al fine di evitare un generale "assenteismo virtuale" è consentita durante la pausa pranzo solo tramite dispositivi personali.

10.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, *Sviluppo Toscana* rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano l'accesso a determinati siti inseriti in una black list o a deteminati tipi di file.

10.4 Gli eventuali controlli, compiuti dal personale incaricato del Servizio ICT ai sensi del precedente punto 3.3, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 30 giorni, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

11. Protezione antivirus

11.1 Il sistema informatico di Sviluppo Toscana è protetto da software antivirus secondo le politiche del fornitore. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

11.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del Servizio ICT.

11.3 Ogni dispositivo magnetico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio ICT.

12. Utilizzo dei telefoni, fax e fotocopiatrici aziendali

12.1 **Il telefono aziendale affidato all'utente è uno strumento di lavoro.** Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa.

La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso aziendale a disposizione dipendente/collaboratore.

12.2 Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal personale del Servizio ICT.

12.3 È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.

12.4 È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

12.5 Nel caso di smarrimento del cellulare aziendale, soprattutto se lo stesso è utilizzato per la lettura della posta elettronica, è necessario fare riferimento alle indicazioni del DPO relative allo smarrimento, furto, distruzione danneggiamento della strumentazione di lavoro allegato alla presente policy.

12.6 E vietato configurare la posta elettronica aziendale su telefoni personali, nonché memorizzare in modo permanente le credenziali di accesso a risorse aziendali su telefoni personali.

13. Osservanza delle disposizioni in materia di Privacy

13.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come alla disposizione dell'AU reperibile sulla pagina aziendale http://www.sviluppo.toscana.it/protezione_dati_personali

14. Accesso ai dati trattati dall'utente

14.1 Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Aziendale, tramite il personale del Servizio ICT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

15. Sistemi di controlli graduali

15.1 In caso di anomalie, il personale incaricato del servizio ICT effettuerà controlli anonimi che si concluderanno con un avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base individuale potranno essere computi solo in caso di successive ulteriori anomalie.

15.2 In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

16. Sanzioni

16.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, nonché con tutte le azioni civili e penali consentite.

17. Aggiornamento e revisione

17.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dalla Direzione Generale.

Firenze, 24 Ottobre 2019

L'Amministratore Unico

Allegato 1

Indicazioni del Data Protection Officer

Smarrimento, furto e distruzione di strumentazioni di lavoro

A tutti i dipendenti e a tutti coloro, coinvolti nel trattamento di dati personali, che operano negli uffici di Sviluppo Toscana S.p.A.

Il Regolamento UE 2016/679 sulla protezione dei dati personali, prescrive che il titolare del trattamento è tenuto a garantire, mediante l'adozione di specifiche misure tecniche e organizzative, un'adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. Qualora si verifichino delle violazioni della sicurezza che comportano 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, il titolare ha l'obbligo di registrare l'evento in un apposito registro, nonché nei casi più gravi di notificare la violazione all'Autorità di controllo e se il rischio della violazione è molto elevato anche agli interessati coinvolti."

Pertanto, si da indicazione a tutto il personale, onde evitare che il verificarsi accidentale di eventi quali lo smarrimento, il furto e la distruzione di strumentazioni di lavoro (ad es. portatili, tablet, chiavette usb, dischi di memoria esterni, smartphone) esponga il titolare a tali rischi, a non salvare files e documenti contenenti dati personali in locale, ma di effettuare il salvataggio sempre sui dischi di rete. Qualora tale necessità fosse indispensabile, accertarsi che i trattamenti derivanti dall'uso dei dati gestisti in locale, siano presenti nel registro dei trattamenti con indicazione dell'asset (stazione di lavoro, o altro supporto di archiviazione), dove vengono registrati e trattati.

Si raccomanda in particolare l'adozione di tale accorgimento ai dipendenti tele-lavoratori, che proprio in virtù della loro modalità di prestazione lavorativa sono più esposti ad incorrere in tali evenienze.

Nel caso in cui tali eventi (furti, smarrimenti, distruzioni) si verifichino, occorre che il lavoratore, dopo aver provveduto alle denunce e segnalazioni d'obbligo, rilasci una dichiarazione al Direttore in quanto titolare del trattamento o direttamente all'Ufficio DPO, nella quale dia atto se nello strumento oggetto di smarrimento, furto o distruzione vi fossero dati personali salvati in locale, e se sì quali, in relazione alla loro tipologia (dati comuni, dati particolari, dati sanitari, dati giudiziari), alle categorie di persone (interessati) a cui si riferiscono, alla loro numerosità e se possibile i contatti di dette persone.

A tal fine si rende disponibile, in allegato, un modello di dichiarazione.

Data Protection Officer
Dott. Giancarlo Galardi

DICHIARAZIONE SOSTITUTIVA DI ATTO DI NOTORIETÀ

(rilasciata ai sensi dell'art. 47 del DPR n. 445 del 28/12/2000)

Il/La sottoscritto/a _____

nr. matricola _____

assegnato/a al settore _____

Ente SVILUPPO TOSCANA S.p.A.

consapevole delle sanzioni penali e civili, nel caso di dichiarazioni mendaci, di formazione o uso di atti falsi, richiamate dall'art. 76 del DPR n. 445 del 28/12/2000, sotto la propria responsabilità

DICHIARA

☐ che nello strumento oggetto di smarrimento, furto o distruzione non vi erano dati personali

☐ che nello strumento oggetto di smarrimento, furto o distruzione vi erano dati personali salvati in locale che nel dettaglio riguardano i seguenti:

a) attività di trattamento: Previste nel registro dei trattamenti ☐
NON previste nel registro dei trattamenti ☐

(descrizione o indicazione nr. Trattamento nel registro)

_____
_____
_____
_____

b) tipi di dati: (comuni; particolari; giudiziari …):

_____
_____
_____

c) categorie di interessati e loro numerosità:

_____
_____

d) ulteriori notizie utili sul trattamento dei dati :

_____
_____

_____ _____

luogo e data firma del dichiarante

Ai sensi dell'articolo 13 del Reg. UE/679/2016 La informiamo che i suoi dati personali, che raccogliamo al fine di valutare una possibile notificazione di violazione di sicurezza all'Autorità di controllo (art. 33 GDPR), saranno trattati in modo lecito, corretto e trasparente.
A tal fine le facciamo presente che:
1. Sviluppo Toscana S.p.A. è il titolare del trattamento (dati di contatto: ufficiodpo@sviluppo.toscana.it)
2. Il conferimento dei suoi dati, che saranno trattati dal personale autorizzato con modalità manuale e informatizzata, è obbligatorio e il loro mancato conferimento preclude gli adempimenti successivi obbligatori per legge. I dati raccolti non saranno oggetto di comunicazione a terzi, se non per obbligo di legge e non saranno oggetto di diffusione.
3. I suoi dati saranno conservati presso gli uffici del Responsabile della protezione dei dati per il tempo necessario alla conclusione del procedimento stesso, saranno poi conservati in conformità alle norme sulla conservazione della documentazione amministrativa.
4. Lei ha il diritto di accedere ai dati personali che la riguardano, di chiederne la rettifica, la limitazione o la cancellazione se incompleti, erronei o raccolti in violazione della legge, nonché di opporsi al loro trattamento per motivi legittimi rivolgendo le richieste al Responsabile della protezione dei dati (urp_*dpo@regione.toscana.it)*.
***5. Può inoltre proporre reclamo al Garante per la protezione dei dati personali,* come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento)**