Capital Security Srls

La corretta gestione della Presa di Servizio dal punto di vista della Privacy e del GDPR

Corso online tenuto in data 28/08/2023

Relatore: Dott. Giancarlo Favero - Direttore

Capital Security Srls
Via Montenapoleone 8 – 20121 Milano
Via Scarlatti, 7 – 20124 Milano

www.capitalsecurity.it

Comunicazioni di Servizio

- L'evento sarà registrato, ed il link per rivedere l'evento registrato sarà pubblicato sul Forum di Capital Security: https://www.capitalsecurity.it/phpbb/viewforum.php?f=2
- Per richiedere gli attestati di partecipazione mandare una mail ad

amministrazione@capitalsecurity.it

specificando Istituto di appartenenza (compresa la città) ed elenco dei partecipanti (nome e cognome)

Capital Security Srls
Via Montenapoleone, 8
Milano

Presa di servizio: alcuni quesiti frequenti

- Siamo sicuri che dobbiamo acquisire tutti quei dati ?
- Siamo sicuri che abbiamo il diritto/potere/titolo ad acquisire tutti quei dati ?
- Che cosa si rischia se si acquisiscono dati eccedenti o senza averne titolo ?
- La ragioneria territoriale chiede che la Scuola invii i casellari giudiziali: glieli possiamo inviare ?
- Quali sono i principi chiave che dobbiamo seguire per non commettere errori ?
- E' possibile eliminare il cartaceo ?
- E' possibile utilizzare la firma grafometrica ?

Capital Security Srls
Via Montenapoleone, 8
Milano

Presa di servizio: alcuni quesiti frequenti

- Dobbiamo predisporre una informativa specifica ? Dobbiamo predisporre più informative ?
- Dobbiamo acquisire dei consensi al trattamento dei dati oppure qualche liberatoria particolare ?
- Possiamo utilizzare un'unica nomina ad incaricato del trattamento dei dati oppure dobbiamo predisporre differenti nomine ad incaricato del trattamento dei dati ?
- Vi sono modalità semplificate per la designazione degli incaricati ?
- Quali altri documenti dobbiamo consegnare/rendere disponibili al dipendente all'atto della presa di servizio ?

Capital Security Srls
Via Montenapoleone, 8
Milano

Peculiarità della Presa di Servizio

- Elevata intensità di acquisizione dati: in pochissimo tempo (un giorno) vengono acquisiti moltissimi dati
- Elevata «pericolosità/delicatezza» dei dati trattati: es. vaccinazioni effettuate, certificazione «antipedofilia», casellario giudiziale etc.
- Spesso qualcuno obietta che il Dirigente Scolastico non ha titolo, non ha il potere o l'autorizzazione ad acquisire/trattare certe tipologie di dati

Capital Security Srls
Via Montenapoleone, 8
Milano

Considerazioni generali

- L'impressione generale è che il processo si basi su modulistica e prassi obsolete
- Vi potrebbe essere acquisizione di dati eccedenti o inutili, in quanto già acquisiti mediante piattaforme web (es Pass Web)
- Talvolta vi sono problemi di «sincronizzazione» del processo
- Si fanno dei ragionamenti sbagliati: «è su format del Ministero…», «ce lo chiede il Ministero….», «ce lo chiede la ragioneria territoriale» : ciò non esime dall'applicare il principio di minimizzazione dei dati ed il principio di liceità

Capital Security Srls
Via Montenapoleone, 8
Milano

Quali sono i principi chiave che dobbiamo seguire per non commettere errori ?

Principio di MINIMIZZAZIONE DEI DATI

- Rif. GDPR Art. 5 comma 1 lettera c): I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati
- Non bisogna acquisire/trattare dati eccedenti rispetto a quelli indispensabili per il perseguimento delle finalità
- Non bisogna acquisire dati in anticipo rispetto al momento in cui l'acquisizione diventerà indispensabile
- I dati acquisiti ed effettivamente utilizzati nel procedimento devono essere esatti

Capital Security Srls
Via Montenapoleone, 8
Milano

Conseguenze del mancato rispetto del principio di minimizzazione

- Acquisizione di dati eccedenti:
  - Aumento della complessità del processo
  - Aumento dei costi, soprattutto se il processo viene gestito in modalità cartacea
  - Aumento dei rischi
  - Aumento del rischio di violazioni dei dati

Capital Security Srls
Via Montenapoleone, 8
Milano

Principio di LICEITA'

- Prima del GDPR: I soggetti pubblici possono trattare dati personali solo per lo svolgimento delle funzioni istituzionali
- Dopo il GDPR: I soggetti pubblici possono trattare dati personali solo se il trattamento è previsto da norma di legge
- Dopo il GDPR e dopo il decreto-legge 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla legge 3 dicembre 2021, n. 205: La base giuridica del trattamento effettuato dai soggetti pubblici è costituita da disposizioni di legge O DA ATTI AMMINISTRATIVI GENERALI (es. circolari ministeriali)

Capital Security Srls
Via Montenapoleone, 8
Milano

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Capo II - *Principi*

Art. 2-*ter* (*Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*)

1. La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento e' costituita da una norma di legge o di regolamento o da atti amministrativi generali.[2]

1-bis. Fermo restando ogni altro obbligo previsto dal Regolamento e dal presente codice, il trattamento dei dati personali da parte di un'amministrazione pubblica di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, ivi comprese le autorità indipendenti e le amministrazioni inserite nell'elenco di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, nonché da parte di una società a controllo pubblico statale o, limitatamente ai gestori di servizi pubblici, locale, di cui all' articolo 16 del testo unico in materia di società a partecipazione pubblica, di cui al decreto legislativo 19 agosto 2016, n. 175 , con esclusione, per le società a controllo pubblico, dei trattamenti correlati ad attività svolte in regime di libero mercato, è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti. In modo da assicurare che tale esercizio non possa arrecare un pregiudizio effettivo e concreto alla tutela dei diritti e delle libertà degli interessati, le disposizioni di cui al presente comma sono esercitate nel rispetto dell' articolo 6 del Regolamento. [3]

2. La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri e' ammessa se prevista ai sensi del comma 1 o se necessaria ai sensi del comma 1-bis. [4]

3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalita' sono ammesse unicamente se previste ai sensi del comma 1 o se

Capital Security Srls
Via Montenapoleone, 8
Milano

servizi, il trattamento dei dati personali del minore di eta' inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, e' lecito a condizione che sia prestato da chi esercita la responsabilita' genitoriale.

2. In relazione all'offerta diretta ai minori dei servizi di cui al comma 1, il titolare del trattamento redige con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo, le informazioni e le comunicazioni relative al trattamento che lo riguardi.

Art. 2-*sexies* *(Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante)*

1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonche' le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. [6]

[6] Comma così modificato dal decreto-legge 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla legge 3 dicembre 2021, n. 205, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché

Presa di servizio: alcuni quesiti frequenti

- ***Dobbiamo predisporre una informativa specifica ? Dobbiamo predisporre più informative ?***
- ***Dobbiamo acquisire dei consensi al trattamento dei dati oppure qualche liberatoria particolare ?***
- Possiamo utilizzare un'unica nomina ad incaricato del trattamento dei dati oppure dobbiamo predisporre differenti nomine ad incaricato del trattamento dei dati ?
- Vi sono modalità semplificate per la designazione degli incaricati
- Quali altri documenti dobbiamo consegnare/rendere disponibili al dipendente all'atto della presa di servizio ?

Capital Security Srls
Via Montenapoleone, 8
Milano

Le informative di parecchie Scuole sono fuori legge

- Art 12 comma 1 del GDPR: l'informativa deve essere CONCISA
- CONCISA significa… **CONCISA**!!
- Qualsiasi informativa più lunga di due pagine viola l'art. 12 comma 1 del GDPR, la qual cosa è punibile con la sanzione fino a 20.000.000,00 Euro ai sensi dell'art. 83 comma 5 lettera b) del GDPR
- Perché alcune informative sono molto lunghe ?

Capital Security Srls
Via Montenapoleone, 8
Milano

Il 99% delle informative delle Scuole sono fuori legge

- Alcune informative sono molto lunghe perché spesso non si conosce la materia
- Il GDPR ha introdotto delle semplificazioni
- Ad esempio non è più necessario specificare le MODALITA' del trattamento, o i luoghi di trattamento
- Con i luoghi di trattamento si rischia di fare delle dichiarazioni false (es. «*I dati saranno trattati nei locali dell'Istituto*»)
- Altra affermazione falsa: i dati non saranno comunicati a paesi terzi

Capital Security Srls
Via Montenapoleone, 8
Milano

Presa di servizio: alcuni quesiti frequenti

- ***Dobbiamo predisporre una informativa specifica ?***

  No, in generale non è necessario predisporre un'informativa specifica

- ***Dobbiamo predisporre più informative ?***

  No, non è necessario predisporre più informative

- ***Dobbiamo acquisire dei consensi al trattamento dei dati oppure qualche liberatoria particolare ?***

  No, non è necessario acquisire il consenso al trattamento dei dati o gestire liberatorie particolari

Capital Security Srls
Via Montenapoleone, 8
Milano

Presa di servizio: alcuni quesiti frequenti

- Dobbiamo predisporre una informativa specifica ? Dobbiamo predisporre più informative ?
- Dobbiamo acquisire dei consensi al trattamento dei dati oppure qualche liberatoria particolare ?
- ***Possiamo utilizzare un'unica nomina ad incaricato del trattamento dei dati oppure dobbiamo predisporre differenti nomine ad incaricato del trattamento dei dati ?***
- ***Vi sono modalità semplificate per la designazione degli incaricati***
- ***Quali altri documenti dobbiamo consegnare/rendere disponibili al dipendente all'atto della presa di servizio ?***

Capital Security Srls
Via Montenapoleone, 8
Milano

<< Intestazione dell'Istituto>>
<< Dati di contatto dell'Istituto>>

Data:

Oggetto: Decreto del Dirigente Scolastico per la designazione cumulativa degli incaricati al trattamento dei dati, ai sensi degli artt. 29 e 32 del GDPR

Prot:

IL DIRIGENTE SCOLASTICO

PREMESSO che ai sensi ed in ottemperanza a quanto previsto dall'art. 29 del Reg. UE 2016/679 (GDPR), chiunque abbia accesso ai dati personali ed effettui operazioni di trattamento deve essere esplicitamente designato, autorizzato ed istruito;

CONSIDERATO che la designazione può fare riferimento all'appartenenza ad un determinato livello organizzativo;

CONSIDERATO che l'art. 32 comma 1 del GDPR prevede che il Titolare del trattamento debba mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio;

CONSIDERATA la necessità di assicurare un adeguato livello di sicurezza e di protezione

CONSIDERATO che l'art. 32 comma 1 del GDPR prevede che il Titolare del trattamento debba mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio;

CONSIDERATA la necessità di assicurare un adeguato livello di sicurezza e di protezione dei dati personali e dei trattamenti connessi, nonché la piena conformità al contesto normativo vigente in materia di sicurezza e protezione dei dati personali;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), di seguito Regolamento;

VISTO il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, così come modificato dal decreto legislativo 10 agosto 2018, n. 101, di seguito Codice;

TUTTO QUANTO SOPRA VISTO E PREMESSO

TUTTO QUANTO SOPRA VISTO E PREMESSO

IL DIRIGENTE SCOLASTICO DECRETA QUANTO SEGUE:

- tutti i dipendenti dell'Ente (personale Docente, Personale ATA etc.) sono designati ed autorizzati, ai sensi degli artt. 29 e 32 del GDPR, a trattare i dati personali e particolari che risulteranno essere necessari per lo svolgimento dei compiti istituzionali e delle mansioni affidate, e pertanto assumono la qualifica di "***Incaricati del trattamento***";
- tutto il personale dipendente dell'Ente, opportunamente designato ed autorizzato ai sensi degli artt. 29 e 32 del GDPR, in tutte le operazioni di trattamento dei dati è tenuto a seguire scrupolosamente le istruzioni consultabili ai seguenti link:
  - ***Istruzioni Generali sul Trattamento dei Dati***: <<inserire link al documento GDPR Scuole - DOC013-A- Nomina Incaricato - Solo istruzioni Ver 9-0>>
  - ***Regolamento per il corretto utilizzo di Internet, della posta elettronica e degli strumenti informatici e telematici*** <<inserire link al documento GDPR Scuole - DOC019 - Regolamento Internet Ver 9-0>>
  - ***Regolamento per il riutilizzo e lo smaltimento di apparecchiature elettroniche e supporti di memorizzazione*** <<inserire link al documento GDPR Scuole - DOC004 - REGRiutilizzoSmaltimento PC Ver 9-0 >>
- la mancata osservanza delle istruzioni di cui al punto precedente potrà comportare sanzioni civili, penali, amministrative e disciplinari;
- l'informativa ai sensi dell'art. 13 del GDPR per il personale dipendente può essere visionata consultando il seguente link: <<inserire link al documento GDPR Scuole – DOC

Via Montenapoleone, 8
Milano

- ***Regolamento per il riutilizzo e lo smaltimento di apparecchiature elettroniche e supporti di memorizzazione*** <<inserire link al documento GDPR Scuole - DOC004 - REGRiutilizzoSmaltimento PC Ver 9-0 >>

- la mancata osservanza delle istruzioni di cui al punto precedente potrà comportare sanzioni civili, penali, amministrative e disciplinari;
- l'informativa ai sensi dell'art. 13 del GDPR per il personale dipendente può essere visionata consultando il seguente link: <<inserire link al documento GDPR Scuole – DOC GDPR Scuole - DOC007 - Informativa Dipendenti - Ver 9-0>>
- per qualsiasi dubbio o chiarimento relativamente alle succitate istruzioni e regolamenti, è possibile rivolgersi al Dirigente Scolastico o al Responsabile della protezione dei dati designato dall'Istituto ai sensi dell'art. 37 del GDPR, Dott. Giancarlo Favero, che può essere contattato ai numeri 02-94750267 o 335-5950674, oppure alla mail giancarlo.favero@capitalsecurity.it, oppure ponendo un quesito all'interno del Forum di discussione https://www.capitalsecurity.it/phpbb/viewforum.php?f=2.

Luogo e data .....

Il Dirigente Scolastico

_____

Via Montenapoleone, 8
Milano

Problemi di «sincronizzazione» del processo

- Trattare dati personali equivale a manipolare armi ed esplosivi (attività pericolose - Art. 2050 del Codice Civile)
- Già il giorno successivo il dipendente (ed esempio un docente) potrebbe trattare dati personali
- Se il dipendente tratta dati personali senza essere autorizzato e senza avere ricevuto le istruzioni, il Dirigente Scolastico è in difetto ed è sanzionabile, per violazione dell'art. 29 del GDPR
- Se viene creato un qualsiasi account senza prima aver nominato (e quindi autorizzato ed istruito) il dipendente, il DS è sanzionabile
- La violazione dell'art. 29 del GDPR è punibile con la sanzione amministrativa pecuniaria fino a 10.000.000,00 Euro, ed espone il DS a problematiche di natura giuslavoristica e sindacale

Capital Security Srls
Via Montenapoleone, 8
Milano

Problemi di «sincronizzazione» del processo: casi reali

- Assistente amministrativo che invia una mail ai genitori, senza utilizzare il ccn (o bcc)
- Violazione dei dati piuttosto grave che non viene tempestivamente segnalata al DS e al DPO
- Docente che non utilizza correttamente il Registro Elettronico

Capital Security Srls
Via Montenapoleone, 8
Milano

Problemi di «sincronizzazione» del processo: una proposta

Io sottoscritto Mario Rossi, nato a _____ il_____, dichiaro che in data 01/09/2023 ho preso servizio presso l'Istituto xxx.

Dichiaro inoltre:

- di avere ricevuto copia del Decreto del Dirigente Scolastico del _____ Prot ____ relativo alla designazione degli incaricati del trattamento;
- di essere consapevole che come conseguenza del succitato Decreto, con la presa di servizio il sottoscritto assume automaticamente e con effetto immediato la qualifica di "incaricato al trattamento" ai sensi dell'art. 29 del Reg. UE;
- di essere consapevole che con la presa di servizio il sottoscritto è tenuto ad osservare e mettere in pratica le istruzioni contenute nel succitato decreto, sin da subito, in tutte le operazioni di trattamento dei dati.

Capital Security Srls
Via Montenapoleone, 8
Milano

Richieste eccedenti da parte della ragioneria territoriale

- Talvolta la ragioneria territoriale chiede alla Scuola di trasmettere il Casellario Giudiziale ed il certificato dei carichi pendenti
- La Scuola deve in ogni caso valutare se la richiesta sia lecita ed applicare in ogni caso i principi di cui all'art. 5 del GDPR, con particolare riferimento al principio di minimizzazione dei dati ed al principio di liceità
- Inoltre, la Scuola deve avere una ragionevole certezza che i dati richiesti siano indispensabili per lo svolgimento delle funzioni istituzionali
- Per quanto sopra esposto, a nostro avviso la richiesta della ragioneria **NON** deve essere soddisfatta

Capital Security Srls
Via Montenapoleone, 8
Milano

L’utilizzo della firma grafometrica

- Non si può imporre l’utilizzo della firma grafometrica: l’interessato (dipendente, genitore etc.) deve esplicitamente accettare l’utilizzo della firma grafometrica
- Per la firma grafometrica deve essere predisposta una specifica informativa
- Attenzione alla robustezza ed alla effettiva validità della firma grafometrica
- In qualsiasi momento l’utente può comunicare che non intende più utilizzare la firma grafometrica
- Attenzione che alcuni gestori di RE stanno dando istruzioni non corrette («identificare l’utente trattenendo copia di un documento di riconoscimento»)

Capital Security Srls
Via Montenapoleone, 8
Milano

Grazie per l'attenzione

Relatore Dott. Giancarlo Favero

Tel. 02-94750267 Cell. 335-5950674

mail giancarlo.favero@capitalsecurity.it

amministrazione@capitalsecurity.it

www.capitalsecurity.it

Capital Security Srls
Via Montenapoleone, 8
Milano