VADEMECUM IN INFORMACIJE O OBDELAVI OSEBNIH PODATKOV

Šole morajo pri opravljanju svojih nalog spoštovati zasebnost in varovati osebne podatke, ki jih obdelujejo, tudi ob upoštevanju dejstva, da med temi podatki obstajajo podatki mladoletnih oseb. Obdelava podatkov s strani izobraževalnih ustanov je upravičena zaradi pomembnega javnega interesa. Obdelava osebnih podatkov pomeni vsako dejanje, opravljeno tudi s pomočjo računalniških orodij, ki zadeva zbiranje, evidentiranje, pregledovanje, obdelavo, uporabo, razširjanje in izbris podatkov. Zakonodajni odlok 196/2003 določa pravila za obdelavo osebnih podatkov za statistične, znanstvene ali zgodovinske namene.

Člen 2 sexies Zakona o varstvu osebnih podatkov (Zakon 196/2003) v posodobljeni obliki določa, da: „Javni interes se šteje za pomemben v primeru obdelave, ki jo opravljajo subjekti, ki izvajajo naloge v imenu javnega interesa ali so povezane z izvrševanjem javnih pooblastil na naslednjih področjih: izobraževanje in usposabljanje v šolah, v poklicu, v visokem šolstvu ali univerzitetnem izobraževanju“.

Zato lahko javne šole obdelujejo le osebne podatke, ki so potrebni za doseganje posebnih institucionalnih ciljev, ki so vsekakor v pomembnem javnem interesu.

Zlasti se za pomembne v javnem interesu štejejo podatki o šolskih, vmesnih in končnih rezultatih za namene, povezane s šolskim in univerzitetnim izobraževanjem.

Tako javne kot zasebne šole so dolžne zadevnim osebam (z ustreznim obvestilom) sporočiti značilnosti in načine obdelave njihovih podatkov ter navesti odgovorne za obdelavo. Zadevne osebe niso le učenci, ampak tudi družine in učitelji. Pomembno je tudi, da šole preverijo svojo obdelavo in nadzorujejo, da podatki niso preseženi glede na namene, za katere se zbirajo.

Podatki, ki niso pomembni za institucionalne namene, se ne smejo zahtevati. Za takšno obdelavo torej ni potrebno soglasje učencev, saj je pravna podlaga za obdelavo javni interes. Vendar je pri obdelavi podatkov potrebna posebna previdnost, saj gre za podatke o osebah, ki so na splošno mladoletne. V nekaterih primerih gre tudi za podatke, ki so predmet posebne obdelave, tj. podatki o zdravju ali sodni podatki. V tem primeru je treba ravnati z največjo previdnostjo in predvsem preveriti, ali je obdelava teh podatkov resnično potrebna za doseganje šolskih ciljev.

Znanje o podatkih invalidnih učencev ali učencev z učnimi težavami mora biti omejeno na določene osebe, kot so učitelji, starši in zdravstveni delavci, ki morajo skupaj pripraviti individualiziran izobraževalni načrt (Zakon št. 104/92, Zakon št. 328/2000 in Zakonski odlok št. 66/2017).

Osebe, vključene v obdelavo osebnih podatkov

Upravljavec

V šoli je ravnatelj tisti, ki določi namene in sredstva obdelave osebnih podatkov in deluje kot garant varnosti.

Naloge upravljavca so:

- sodelovanje pri vodenju evidence dejavnosti obdelave;
- usklajevanje posodabljanja obvestil o zasebnosti, ki jih je treba posredovati zainteresiranim osebam;
- nadzorovanje osebja, ki je odgovorno za obdelavo podatkov;
- zagotavljanje takojšnjega odgovora na zahteve pooblaščenca za varstvo podatkov, ki se nanašajo na njegovo področje delovanja
- usklajevanje, od trenutka načrtovanja postopkov obdelave in uporabe informacijskih aplikacij, dejavnosti za preverjanje vpliva na zasebnost posameznikov, na katere se nanašajo osebni podatki,.

V skladu z zakonskim odlokom 196/2003 je ravnatelj, kot upravljavec osebnih podatkov učencev in staršev, dolžan pooblastiti osebje za obdelavo podatkov pri opravljanju posebnih nalog. Brez tega pooblastila v teoriji ne bi bilo mogoče obdelovati osebnih podatkov učencev, kar bi povzročilo zastoj dejavnosti šole.

Za administrativno osebje ravnatelj imenuje vodjo uprave za „odgovornega za obdelavo“, ki organizira obdelavo podatkov v skladu z Zakonom o varstvu osebnih podatkov (Zakon 196/2003) in uredbo o občutljivih in sodnih podatkih. Ob imenovanju vodja uprave prejme od ravnatelja pooblastilo, da med administrativnim osebjem določi osebe, odgovorne za obdelavo. Za učitelje sestavi skupno pismo, v katerem jih pooblasti za obdelavo osebnih podatkov učencev. Pismo je priloženo temu obvestilu.

Odgovorna oseba za obdelavo

Je fizična ali pravna oseba, ločena od upravljavca, ki obdeluje osebne podatke v imenu upravljavca in pod njegovim nadzorom.

Vsak zunanji subjekt, ki obdeluje osebne podatke, povezane s šolo, prevzema odgovornost za obdelavo in mora izvajati tehnične ukrepe za zaščito pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki. Naloga mora biti formalizirana z navedbo obveznosti, omejitev in navodil v zvezi z obdelavo v pogodbi, ki izpolnjuje zahteve veljavne zakonodaje. V nekaterih primerih je lahko odgovorna oseba za obdelavo podatkov odgovorna tudi nadzornemu organu.

Notranji odgovorni za obdelavo osebnih podatkov je vodja uprave.

Odgovorni za varstvo podatkov

V skladu z Uredbo EU iz leta 2016 (o obdelavi osebnih podatkov) mora vsaka šola imenovati odgovornega za varstvo podatkov, ki je svetovalna oseba s posebnim pravnim in informacijskim znanjem na področju varstva podatkov, ki nadzira in podpira ravnatelja in vodjo uprave, da zagotovi izvajanje obdelave podatkov v skladu z Zakonom o varstvu osebnih podatkov in Uredbo EU 2016.

Gre za popolnoma avtonomno in neodvisno osebo, tudi od upravljavca, ki ne sme dajati navodil. Upravljavec mora pooblaščencu za varstvo podatkov zagotoviti le sredstva, potrebna za pravilno opravljanje njegovih nalog.

Dostop do podatkov

Za informacije in podatke, ki jih hrani šolska ustanova, ter za uveljavljanje pravice do popravka in popravljanja se lahko obrnete na upravljavca, ki je običajno ista šolska ustanova. V primeru neodzivnosti se lahko obrnete do varuha zasebnosti ali sodstvo. Kar zadeva posamezne upravne akte, je mogoče dostopati do dokumentacije o učencih in študentih v skladu z zakonom 241 iz leta 1990 (členi 22 in naslednji). V tem primeru mora šola presoditi, ali ima prosilec neposreden, konkreten in aktualen interes za pridobitev zadevnega akta v skladu z veljavno zakonodajo o dostopu do aktov javne uprave.

Register obdelave

Šole morajo voditi register obdelave. Ministrstvo za šolstvo, z uradnim obvestilom št. 877 z dne 03.08.2018, je šolam posredovalo „Vzorec registra dejavnosti obdelave“ za izobraževalne ustanove, ki ga predpisuje Evropska uredba o obdelavi osebnih podatkov. Priloženo je tudi operativno vodilo, ki pojasnjuje metodologijo za izpolnjevanje registra. V priročniku so navedene nekatere osnovne obdelave za upravljanje dokumentov v zvezi s postopki, ki se običajno izvajajo v šolah. Podrobno jih preučimo.

Dejavnosti obdelave

Šole morajo opraviti 6 dejavnosti obdelave, ki so podrobno opisane v Excelovi datoteki z naslovom: „Register obdelav – primer izpolnjevanja“. V metodološkem opisu ministrstvo navaja primere naslednjih postopkov:

Upravljanje vpisov
Upravljanje šolske kariere učencev
Upravljanje učnega osebja – sklepanje pogodb

Upravljanje vpisov

Vpis v šolo, od osnovne do srednje, poteka elektronsko, tj. prek spletne strani MIM. V zvezi z vpisom so bile glede na kategorijo obdelanih podatkov (npr. posebne kategorije osebnih podatkov), namene obdelave (npr. priprava razvrstitev, razvrščanje in sprejemanje vpisnih prošenj ali dokončanje vpisa), vrsto in način obdelave (npr. aplikacija SIDI ali lokalni paket) opredeljene tri dejavnosti:

1. Pridobivanje in upravljanje vlog 2. Pridobivanje dodatne dokumentacije 3. Pridobivanje in upravljanje vlog

Ta dejavnost vključuje zbiranje prijav, predloženih na spletu ali v papirni obliki, kjer je to predvideno, in njihovo upravljanje za pripravo razvrstitev, sprejemanje ali razvrščanje vlog za vpis na podlagi razpoložljivih mest in meril za prednost, ki jih določi šolski svet.

Če šola uporablja funkcije portala SIDI:

Ministrstvo je zunanji odgovorni za obdelavo, saj je javni organ, ki prek razpoložljive aplikacije obdeluje osebne podatke v imenu upravljavca, ki je v tem primeru izključno šolska ustanova.

Od šolskega leta 2023/2024 so družine, učitelji, učenci in administrativno osebje seznanjeni z UNICA in delujejo v skladu z njim, v zvezi s čimer je priloženo pojasnilo o varstvu osebnih podatkov, ki ga je pripravilo ministrstvo za šolstvo in zaslužnost (MIM)

https://unica.istruzione.gov.it/it/privacy

Tudi INVALSI vsako leto posreduje družinam obvestilo o varstvu osebnih podatkov za nacionalne teste Invalsi.

Pridobivanje dodatne dokumentacije

Ta dejavnost vključuje zbiranje dokumentacije (obvezne ali neobvezne) za dokončanje vpisa in nadaljnje upravno vodenje učenca. Zbrani podatki vsebujejo splošne podatke in posebne kategorije osebnih podatkov (npr. zdravstveno stanje, verska, filozofska ali druga prepričanja). Ti podatki se obdelujejo v papirni obliki in/ali z uporabo lokalnih paketov. V tem primeru je zunanji obdelovalec, tj. pravna oseba, ki obdeluje osebne podatke v imenu upravljavca, dobavitelj informacijskih sistemov šole.

Upravljanje šolske kariere učencev

V zvezi s šolsko kariero učencev je opredeljena le ena dejavnost: Upravljanje podatkov učencev

Ta obsega:

- obdelavo osebnih podatkov v zvezi s šolsko, izobraževalno in upravno potjo učenca za upravljanje učenca, tudi v zvezi z zagotavljanjem dodatnih storitev
- posodabljanje Nacionalnega registra študentov za izpolnjevanje obveznosti iz M.U. 692/2017.

Če šola uporablja funkcije portala SIDI:

- Ministrstvo je zunanji upravljavec, saj je javni organ, ki prek razpoložljive aplikacije obdeluje osebne podatke v imenu upravljavca, ki je izključno šolska ustanova.

Če šola uporablja lokalne pakete:

- upravljavec je informacijski ponudnik, ki ga izbere šolska ustanova.

Upravljanje učnega osebja – sklepanje pogodb

Sklepanje pogodb z učnim osebjem zadeva vse dejavnosti obdelave podatkov, ki jih šola izvaja za namene zaposlovanja navedenega osebja.

V zvezi s tem postopkom so bile opredeljene naslednje dejavnosti obdelave:

1. Upravljanje pogodb za nedoločen čas
2. Upravljanje pogodb za določen čas
3. Upravljanje pogodb za kratkotrajno in občasno nadomeščanje

Upravljanje pogodb za nedoločen čas.

Ta dejavnost vključuje obdelavo vseh osebnih podatkov, ki so potrebni za dokončanje zaposlitve učiteljskega osebja za nedoločen čas, z upoštevanjem vidikov, povezanih z pravnim in ekonomskim obravnavanjem ter preverjanjem izpolnjevanja pogojev za zaposlitev.

Zgoraj navedena dejavnost vključuje, v okviru obdelave osebnih podatkov, skupno odgovornost v skladu s členom 26 Uredbe (EU) 2016/679 Ministrstva in šole. Glede na to, da se dejavnost izvaja prek funkcij SIDI, je zunanji odgovorni za obdelavo ponudnik informacijskega sistema Ministrstva.

Upravljanje pogodb za določen čas

Ta dejavnost vključuje obdelavo vseh osebnih podatkov, ki so potrebni za zaposlitev učiteljskega osebja za določen čas, s poudarkom na vidikih pravne in ekonomske obravnave ter preverjanju izpolnjevanja pogojev za zaposlitev. Kot v primeru redno zaposlenega osebja, je za obdelavo zadevnih osebnih podatkov skupno odgovorno ministrstvo in šolska ustanova v skladu s členom 26 Uredbe (EU) 2016/679. Glede na to, da se dejavnost izvaja prek funkcij SIDI, je zunanji upravljavec podatkov dobavitelj informacijskega sistema ministrstva.

Upravljanje pogodb za kratkotrajno in občasno nadomeščanje

Ta dejavnost vključuje obdelavo vseh osebnih podatkov, potrebnih za zaposlovanje učiteljskega osebja za kratkotrajno in občasno nadomeščanje, s poudarkom na pravnih in ekonomskih vidikih ter preverjanju izpolnjevanja pogojev za zaposlitev. Šola je izključni upravljavec zadevnih osebnih podatkov, medtem ko je ministrstvo zunanji upravljavec, saj je javni organ, ki prek aplikacije portala SIDI obdeluje osebne podatke v imenu upravljavca.

Kako poteka upravljanje zasebnosti v primeru uporabe fotografij in kamer

Fotografije učencev

Javne šolske ustanove lahko obdelujejo le osebne podatke, ki so potrebni za doseganje posebnih institucionalnih ciljev ali tiste, ki so izrecno predvideni v sektorski zakonodaji. Za takšno obdelavo niso dolžne pridobiti soglasja učencev ali staršev. V tem smislu se objava fotografij učencev na institucionalnih spletnih straneh ali na družbenih omrežjih, povezanih s šolo, lahko šteje za zakonito, saj med institucionalne dejavnosti sodijo tudi prireditve, kot so gledališke predstave, literarni ali znanstveni festivali, dnevi odprtih vrat, dejavnosti usmerjanja, projekti in šolske dejavnosti. Reprodukcija podatkov pa mora biti v skladu z načelom sorazmernosti in služiti izključno za dokumentiranje pedagoške dejavnosti. Zato naj bi bilo snemanje dogodkov omejeno na skupino, ki izvaja dejavnost, pri čemer je treba izogibati se posnetkom v bližini. Učence je treba vedno snemati v pozitivnih ali konstruktivnih položajih, nikoli v negativnih. Razširjanje slik (na internetu) pa mora biti predmet soglasja staršev.

Kamere v šoli

Namestitev sistemov videonadzora v šolah mora v vsakem primeru zagotavljati pravice učencev. Dovoljena je v primerih, ko je to nujno za zaščito šolskega objekta in premoženja pred vandalizmom, pri čemer je snemanje omejeno na zadevna območja. Seveda je treba prisotnost kamer označiti z ustreznimi tablami, kamere v šoli pa se lahko vklopijo šele po koncu pouka in ne med šolskimi in izvenšolskimi dejavnostmi. Zavod je s tem v zvezi sprejel pravilnik, ki je dostopen na šolski spletni strani.

Upravljanje tveganja kršitve varstva podatkov (Data breach)

UKREPI ZA ODGOVORNOST UPRAVLJAVCEV IN ODGOVORNIH

Kršitev varstva podatkov je naključna ali nezakonita kršitev varstva osebnih podatkov, ki nastane zaradi uničenja, izgube, spremembe, nepooblaščenega dostopa ali razkritja osebnih podatkov, ki so shranjeni ali obdelani. Uredba o varstvu osebnih podatkov močno poudarja „odgovornost“ (accountability) upravljavcev in odgovornih oseb – tj. sprejetje proaktivnega ravnanja, ki dokazuje konkretno sprejetje ukrepov za zagotovitev izvajanja uredbe (zlasti člene 23–25 in celoten poglavje IV uredbe). To je velika novost na področju varstva podatkov, saj se upravljavcem zaupa naloga, da samostojno odločajo o načinih, jamstvih in omejitvah obdelave osebnih podatkov – v skladu z zakonskimi določbami in ob upoštevanju nekaterih posebnih meril, navedenih v uredbi. Prvo od teh meril je povzeto v angleškem izrazu „data protection by default and by design“ (člen 25), tj. potreba po konfiguraciji obdelave tako, da se že na začetku predvidijo nujna jamstva za varstvo pravic posameznikov, ob upoštevanju splošnega konteksta, v katerem poteka obdelava, in tveganj za pravice in svoboščine posameznikov. Vse to mora biti storjeno vnaprej, pred dejanskim obdelovanjem podatkov („tako ob določanju sredstev obdelave kot ob sami obdelavi“, kot navaja člen 25(1) uredbe), in zato zahteva predhodno analizo in zavezo k izvajanju s strani upravljavcev, ki morajo sprejeti vrsto posebnih in dokazljivih ukrepov. Že sama imenovanje „pooblaščenca za varstvo podatkov“ (PVP, ali DPO, če uporabljamo angleško kratico: Data Protection Officer) odraža pristop prevzemanja odgovornosti, ki je značilen za uredbo (glej člen 39), saj je namenjen olajšanju izvajanja uredbe s strani upravljavca/pooblaščenca. Ni naključje, da med naloge DPO sodijo „ozaveščanje in usposabljanje osebja“ ter nadzor nad izvajanjem ocene učinka iz člena 35.

Torej ima upravljavec dve obveznosti: varstvo pravic posameznikov in obvladovanje tveganja kršitve varstva podatkov.

Med temi dejavnostmi je bistveno upravljanje tveganja, povezanega z obdelavo. Slednje je treba razumeti kot tveganje negativnih vplivov na svoboščine in pravice posameznikov, na katere se nanašajo osebni podatki; te vplive je treba analizirati s posebnim postopkom ocene (člena 35–36), ob upoštevanju znanih ali zaznavnih tveganj ter tehničnih in organizacijskih ukrepov (tudi varnostnih), ki jih mora upravljavec sprejeti za zmanjšanje teh tveganj (glej smernice o oceni vpliva na varstvo podatkov, ki jih je sprejela skupina „Člen 29“, dostopne tukaj: www.garanteprivacy.it/regolamentoue/DPIA). Na podlagi te ocene učinka lahko upravljavec samostojno odloči, ali bo začel obdelavo (po sprejetju ustreznih ukrepov za zadostno zmanjšanje tveganja) ali se bo posvetoval s pristojnim nadzornim organom, da pridobi navodila o ravnanju z ostankom tveganja; organ ni pristojen za „odobritev“ obdelave, temveč za navedbo morebitnih dodatnih ukrepov, ki jih mora sprejeti upravljavec, in lahko po potrebi sprejme vse popravne ukrepe v skladu s členom 58: od opozorila upravljavcu do omejitve ali prepovedi obdelave. Torej bo posredovanje nadzornih organov predvsem „ex post“, tj. po samostojnih odločitvah

upravljavca; od 25. maja 2018 so namreč nekatere inštitute, predvidene v direktivi iz leta 1995 in v italijanskem zakoniku, kot so predhodno npr. obvestilo o obdelavi nadzornemu organu in tako imenovana predhodna preveritev (ali predhodni pregled), nadomestili z obveznostjo vodenja evidence obdelave s strani upravljavca/odgovorne osebe in izvajanja ocene vpliva v popolni neodvisnosti, s poznejšim morebitnim posvetovanjem z organom.

V okviru varstva in obvladovanja tveganja se analizirajo glavne obveznosti upravljavca in odgovorne osebe za obdelavo podatkov.

Posodobitev obvestil o varstvu podatkov v šolah

Prva naloga, ki jo je treba opraviti za uskladitev z GDPR (št. 679/206, sprejet 25. maja 2018), je posodobitev obvestil, ki jih je treba posredovati zainteresiranim osebam. Zadostuje, da se obvestilo objavi na spletni strani ustanove. Ta obvestila morajo vsebovati informacije o obdobju hrambe podatkov, pravni podlagi, pravicah posameznika in vseh zahtevah iz členov 12, 13 in 14 v zvezi z obveznostjo obveščanja. Do dopolnjenega 18. leta starosti mladoletniki ne morejo dati soglasja za obdelavo podatkov. Po dopolnjenem 18. letu starosti lahko soglasje da samo neposredno zadevna oseba (niti starši niti oseba, ki je izvajala starševsko varstvo). Soglasje ni obvezno za koriščenje storitev za preprečevanje in svetovanje, ki se zagotavljajo neposredno mladoletnim osebam, kot je svetovalna služba za mladoletne. Za posebno obdelavo podatkov, kot so fotografije, posnetki, avdio in video posnetki, ter njihovo razširjanje je potrebno izrecno soglasje zainteresiranih oseb. V javni upravi je rok hrambe zbranih osebnih podatkov določen s strani Ministrstva za kulturno dediščino in dejavnosti.

Register obdelave

Je register obdelave, katerega vsebina je navedena v čl. 30. Gre za temeljno orodje, ki ni pomembno le za morebitni nadzor s strani nadzornega organa, ampak tudi za pridobitev aktualnega pregleda obdelave v podjetju ali javnem organu, kar je nujno za vsako oceno in analizo tveganja. Register mora biti v pisni obliki, tudi elektronski, in ga je treba na zahtevo predložiti nadzornemu organu. Vodenje tega registra je obvezno za vsa podjetja z najmanj 250 zaposlenimi. Podjetja z manj kot 250 zaposlenimi so izvzeta iz te obveznosti, če obdelava podatkov ne predstavlja tveganja za pravice in svoboščine posameznikov. Šole, ki nenehno obdelujejo podatke, zlasti specifične, morajo voditi ta register: pisni dokument v elektronski obliki, ki ga je treba nenehno posodabljati in predložiti nadzornemu organu v primeru morebitne kontrole. Uporaben je tudi kot popoln pregled trenutnega stanja obdelave za tiste, ki ga sestavljajo. Za vsako dejavnost je treba navesti pravno podlago, postopke obdelave podatkov, način obdelave, vrsto obvestila in morebitno prisotnost zunanjih odgovornih oseb. Register mora vsebovati vsaj:

- Ime in kontaktne podatke upravljavca, sopodatkovnega upravljavca, zastopnika za obdelavo in pooblaščenca za varstvo podatkov
- Namen obdelave
- Opis kategorije posameznikov, na katere se nanašajo osebni podatki, in obdelanih podatkov
- Opis kategorije prejemnikov podatkov, vključno s tretjimi osebami
- Morebitni prenosi podatkov
- Roki za izbris podatkov

- Varnostni ukrepi (tehnični in organizacijski)

To so minimalne informacije, ki jih je treba vpisati v register, vendar je priporočljivo navesti vse druge informacije, ki so koristne za izboljšanje te analize obdelave in s tem povezanih tveganj.

Varnostni ukrepi

Varnostni ukrepi morajo zagotavljati raven varnosti, ki ustreza tveganju obdelave (člen 32, odstavek 1); v tem smislu je seznam iz člena 32, odstavek 1, odprt in ni izčrpen („med drugim, če je to primerno“). Iz istega razloga po 25. maju 2018 ne veljajo več splošne obveznosti sprejetja „minimalnih“ varnostnih ukrepov (v skladu s členom 33 Kodeksa), saj je ta ocena prepuščena posameznim primerom upravljavcu in pooblaščencu v skladu s tveganji, ki so posebej opredeljena v členu 32 Uredbe.

Preprečevanje in upravljanje ocene učinka

Načelo odgovornosti, ki je povečalo odgovornost upravljavca osebnih podatkov, ki mora sprejeti tehnične in organizacijske varnostne ukrepe za varstvo osebnih podatkov, temelječe na načelih „tveganja“. V šolah so tveganja za kršitev varstva podatkov lahko povezana z naslednjimi dejavniki:

- Nepravilno ravnanje (nepozornost, nevednost, goljufivo ravnanje, kraja, izguba) šolskega administrativnega osebja, učiteljev, učencev ali staršev.
- Zunanje in/ali notranje kršitve informacijske varnosti (virusi, zlonamerna programska oprema, sabotaža, prestrezanje, zastarelost, okvara).
- Kršitve v okviru šolske ustanove (nepredvidljivi naravni, namerni, umetni ali naključni dogodki).

Kaj storiti v primeru kršitve varstva podatkov v šoli

V primeru kršitve varstva podatkov mora upravljavec izpolniti tri obveznosti:

- Obvestiti organ za varstvo osebnih podatkov o kršitvi
- Po potrebi obvestiti osebo, na katero se kršitev nanaša
- Posodobiti register kršitev z navedbo okoliščin, posledic in ukrepov, sprejetih za odpravo kršitve.

Od 25. maja 2018 morajo vsi upravljavci nadzornemu organu prijaviti kršitve varstva osebnih podatkov, za katere izvejo, v 72 urah in vsekakor „brez neupravičenega odlašanja“, vendar le, če menijo, da je verjetno, da taka kršitev ogroža pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. Zato obvestilo organu o kršitvi ni obvezno, saj je odvisno od ocene tveganja za posameznike, ki jo mora opraviti upravljavec. Če je verjetnost takšnega tveganja visoka, je treba o kršitvi obvestiti tudi posameznike, in sicer „brez neupravičenega odlašanja“.

Upravljavec mora v vsakem primeru dokumentirati kršitve varstva osebnih podatkov, tudi če niso bile sporočene nadzornemu organu in posameznikom, ter z njimi povezane okoliščine in posledice ter sprejete ukrepe (glej člen 33(5)). Zato mora upravljavec sprejeti potrebne ukrepe za dokumentiranje

morebitnih kršitev, pri čemer je dolžan to dokumentacijo na zahtevo predložiti nadzornemu organu v primeru preiskave.

Ravnanje v primeru izgube ali hekanja občutljivih podatkov

Če zaposleni ugotovi izgubo občutljivih podatkov, ki se nanašajo na osebje ali učence, zaradi izgube ali kraje podatkov, shranjenih na pendrive ali zunanjem trdem disku, mora o tem pisno obvestiti direktorja in navesti način izgube podatkov ter vrsto podatkov. Občutljivi podatki so podatki, ki razkrivajo rasno ali etnično poreklo, verska ali filozofska prepričanja, politična mnenja, sindikalno pripadnost, podatki o zdravju ali spolnem življenju.

Podobno obvestilo je treba poslati, če zaposleni ugotovi, da so bili občutljivi podatki, ki jih ima na uporabljeni napravi, hekani. Zaposleni mora nato predložiti kopijo prijave izgube/kraje, ki je bila poslana lokalni policijski postaji.

Usposabljanje, obveščanje različnih šolskih komponent

Šolsko osebje je vsako leto na začetku leta obveščeno o mehanizmih upravljanja podatkov skladno s poklicnim profilom. Izobraževanje opravlja DPO.

VADEMECUM E INFORMATIVA SUL TRATTAMENTO DATI PERSONALI

Le istituzioni scolastiche, durante lo svolgimento dei loro compiti, hanno il dovere di rispettare la privacy e proteggere i dati personali che trattano, anche in considerazione del fatto che tra questi dati vi sono anche quelli di soggetti minorenni. Il trattamento dei dati da parte delle istituzioni scolastiche è giustificato da motivi di interesse pubblico rilevante. Per trattamento dei dati personali si intende qualsiasi operazione, effettuata anche con l'ausilio di strumenti informatici, concernente la raccolta, la registrazione, la consultazione, l'elaborazione, l'utilizzo, la diffusione e la cancellazione dei dati. Il Dlgs 196/2003 detta le regole per il trattamento dei dati personali, effettuato per scopi statistici, scientifici o storici.

L'art. 2 sexies del Codice Privacy (Dlgs. 196/2003) aggiornato precisa che: "S*i considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie: istruzione e formazione in ambito scolastico, professionale, superiore o universitario*".

Dunque, le scuole pubbliche possono trattare soltanto i dati personali necessari al perseguimento delle specifiche finalità istituzionali, che sono comunque finalità di rilevante interesse pubblico.

In particolare, si considerano di rilevante interesse pubblico i dati relativi agli esiti scolastici, intermedi e finali, per finalità legate alla formazione scolastica e universitaria.

Le scuole, quindi, sia pubbliche che private, hanno l'obbligo di comunicare agli interessati (tramite apposita informativa) le caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento. Gli interessati sono non solo gli studenti, ma anche le famiglie e gli stessi professori. È altresì importante che le scuole verifichino i loro trattamenti, controllando che i dati non siano eccedenti rispetto alle finalità perseguite.

Non possono essere chiesti dati non rilevanti per la finalità istituzionali. Quindi, per tali trattamenti non occorre il consenso degli studenti, la base giuridica del trattamento è, infatti, data dall'interesse pubblico. Occorre, tuttavia, particolare cautela nel trattamento dei dati, trattandosi di dati relativi a soggetti generalmente minorenni. In alcuni casi si tratta anche di dati a trattamento speciale, cioè relativi alla salute o giudiziari. In questo caso le cautele devono essere massime e soprattutto occorre verificare se il trattamento di quei dati sia davvero necessario per il perseguimento delle finalità scolastiche.

La conoscenza di dati di allevi disabili o con disturbi dell'apprendimento deve essere limitata a soggetti specifici, quali docenti, genitori e operatori sanitari che congiuntamente devono predisporre il piano educativo individualizzato (L. n. 104/92, L. n. 328/2000 e D.Lgs. n. 66/2017).

I soggetti coinvolti nel trattamento dei dati personali

Titolare del trattamento

Nella scuola è il Dirigente Scolastico che determina finalità e mezzi del trattamento dei dati personali e funge da garante di sicurezza.

Le funzioni del titolare sono:

- Coadiuvare la tenuta del registro delle attività di trattamento;
- Coordinare l'attività di aggiornamento delle informative da rendere agli interessati;
- Valutare i soggetti inquadrati come responsabili del trattamento;
- Assicurare immediato riscontro alle richieste del RPD riconducibili al settore di appartenenza
- Coordinare le attività di valutazione dell'impatto privacy sugli interessati fin dal momento della progettazione dei processi di trattamento e degli applicativi informatici di supporto.

Ai sensi del Dlgs 196/2003, il DS, in qualità di titolare del trattamento dei dati personali di studenti e genitori, ha l'obbligo di autorizzare il personale al trattamento dei dati, nell'espletamento degli specifici compiti. Senza questa autorizzazione, in teoria, non si potrebbero trattare i dati personali degli alunni, il che comporterebbe un blocco dell'attività della scuola.

Per il personale amministrativo, il DS nomina il DSGA come "responsabile del trattamento", per organizzare le operazioni di trattamento dati nel rispetto del Codice della privacy (Dlgs 196/2003) e del regolamento sui dati sensibili e giudiziari. Nella nomina al DSGA, questi riceve mandato dal DS di individuare tra il personale amministrativo gli incaricati del trattamento. Per i docenti, fa una lettera cumulativa in cui li autorizza al trattamento dei dati personali degli alunni. La lettera è allegata a questa comunicazione.

Responsabile del trattamento

E' una persona fisica o giuridica, distinta dal titolare, che elabora i dati personali per conto del titolare, sotto il suo controllo.

Ogni soggetto esterno alla scuola, se tratta dati personali afferenti alla scuola, si assume la responsabilità trattamento, dovendo mettere in atto misure tecniche a tutela dei diritti e delle libertà degli interessati. L'incarico deve essere formalizzato chiarendo obblighi, limiti e istruzioni riguardanti il trattamento, attraverso un contratto che rispetti i requisiti previsti dalla normativa vigente. Il responsabile del trattamento, in alcuni casi, può essere chiamato a rispondere anche all'autorità di controllo.

Il Responsabile interno del trattamento dei dati personali è il Dsga.

Responsabile della protezione dei dati

Ai sensi del Regolamento UE del 2016 (sul trattamento dei dati personali), ogni scuola deve nominare l'RPD, che è una figura consultiva, con specifiche conoscenze giuridiche e informatiche del settore della protezione dei dati, che vigila e dà supporto al DS e al DSGA al fine di garantire che il servizio di trattamento dei dati avvenga nel rispetto del Codice della privacy e del Regolamento UE 2016.

Si tratta di una figura completamente autonoma e indipendente, anche dal titolare, che non deve dare istruzioni. Il titolare deve solo fornire al RPD le risorse necessarie per il corretto svolgimento delle sue funzioni. L' RPD può essere interno o esterno. Le scuole possono nominare il RPD singolarmente o in rete. Qualora sia interno, la scuola deve garantire che le attività richieste dal ruolo di RPD siano compatibili con le mansioni ordinariamente svolte, per non creare un conflitto di interessi.

Accesso ai dati

Per conoscere le informazioni e i dati conservati dall'istituzione scolastica, ed esercitare, eventualmente, il diritto di rettifica e correzione, è possibile rivolgersi al titolare del trattamento, in genere lo stesso istituto scolastico. In caso di mancata risposta ci si può rivolgere al Garante oppure alla magistratura. Per quanto riguarda, invece, i singoli atti amministrativi, è possibile accedere alla documentazione relativa ad alunni e studenti, in base alla legge 241 del 1990 (artt. 22 e ss). In tal caso, spetta all'istituto valutare se il richiedente ha un interesse diretto, concreto ad attuale ad ottenere l'atto in questione, ai sensi della vigente normativa in materia di accesso agli atti della Pubblica Amministrazione.

Registro dei trattamenti

Le scuole devono tenere il registro dei trattamenti. Il Miur, con nota n. 877 del 03/08/2018, ha trasmesso alle scuole uno "Schema di Registro delle attività di trattamento" per le istituzioni scolastiche, previsto dal Regolamento europeo sul trattamento dei dati personali. fornendo anche una Guida operativa, che illustra la metodologia da applicare per la compilazione del registro. Nella guida, sono indicati alcuni trattamenti di base, per la gestione documentale relativa a processi che si svolgono normalmente nelle scuole. Analizziamole nel dettaglio.

Attività di trattamento

Le attività di trattamento, che devono svolgere le scuole, sono 6 e sono dettagliatamente descritte nel file Excel denominato: "Registro dei Trattamenti Esempio compilazione". Nella nota metodologica, il Ministero riporta esempi relativi ai seguenti processi:

- Gestione iscrizioni
- Gestione carriera scolastica alunni
- Gestione del personale docente – contrattualizzazione

Gestione Iscrizioni

Le iscrizioni a scuola avvengono, dalla primaria alla secondaria, in modalità telematica, ossia online, tramite il sito del MIM. In riferimento alle iscrizioni, in funzione della categoria di dati trattati (ad es. le categorie particolari di dati personali), delle finalità di trattamento (es. predisposizione delle graduatorie, smistamento e accettazione delle domande di iscrizione o perfezionamento dell'iscrizione), della tipologia, e della modalità di trattamento (es. applicativo SIDI o pacchetto locale), sono state individuate due attività:

1.Acquisizione e gestione domande 2. Acquisizione documentazione aggiuntiva 3. Acquisizione e gestione domande

Tale attività prevede la raccolta delle iscrizioni presentate on line o in modalità cartacea, ove previsto, e la gestione delle stesse al fine di predisporre le graduatorie, accettare o smistare le domande di iscrizione sulla base della disponibilità di posti e dei criteri di precedenza deliberati dal Consiglio di Istituto.

<u>Se la scuola utilizza le funzioni del portale SIDI:</u>

- il Ministero è il Responsabile esterno del trattamento, in quanto autorità pubblica che, attraverso l'applicativo messo a disposizione, tratta dati personali per conto del titolare del trattamento, che è in questo caso, in via esclusiva, l'istituzione scolastica.

Dall'a.s.2023/2024, famiglie, docenti, studenti, personale ata hanno conosciuto ed operato con UNICA e a tal proposito si allega quanto precisato in termini di privacy dal MIM

https://unica.istruzione.gov.it/it/privacy

Anche l'INVALSI, annualmente diffonde informativa privacy alle famiglie per le prove Nazionali Invalsi.

Se la scuola utilizza pacchetti locali:

- il responsabile del trattamento è il fornitore informatico scelto dall'istituzione scolastica.

In caso di iscrizioni in modalità cartacea:

- le scuole sono in via esclusiva i titolari del trattamento e non c'è un responsabile esterno del trattamento.

Acquisizione documentazione aggiuntiva

Tale attività prevede la raccolta della documentazione (obbligatoria o facoltativa) per il perfezionamento dell'iscrizione e per la successiva gestione amministrativa dell'alunno. Le informazioni raccolte contengono dati comuni e categorie particolari di dati personali (es. lo stato di salute, le convinzioni religiose, filosofiche o di altro genere). Tali dati sono trattati in modalità cartacea e/o mediante l'utilizzo di pacchetti locali. In tal caso, il Responsabile esterno del trattamento, ovvero la persona giuridica che tratta dati personali per conto del titolare del trattamento, è il fornitore dei sistemi informativi della scuola.

Gestione carriera scolastica alunni

In riferimento alla carriera scolastica degli alunni, l'attività individuata è una soltanto: Gestione dati alunni

Essa consiste:

- nel trattamento di dati personali relativi al percorso scolastico, formativo e amministrativo dell'alunno per la gestione dello studente, anche in relazione all'erogazione di servizi aggiuntivi
- nell'aggiornamento dell'Anagrafe Nazionale degli Studenti al fine di adempiere agli obblighi previsti dal D.M. 692/2017.

Se la scuola utilizza le funzioni del portale SIDI:

- il Ministero è il Responsabile esterno del trattamento, in quanto autorità pubblica che, attraverso l'applicativo messo a disposizione, tratta dati personali per conto del titolare del trattamento, che è, in via esclusiva, l'istituzione scolastica.

Se la scuola utilizza pacchetti locali:

- il responsabile del trattamento è il fornitore informatico scelto dall'istituzione scolastica.

Gestione del personale docente – _contrattualizzazione

La contrattualizzazione del personale docente riguarda tutte le attività di trattamento di dati che sono effettuate dalla scuola ai fini dell'assunzione del predetto personale.

In riferimento a tale processo, sono state individuate le seguenti attività di trattamento:

1. Gestione contratto a tempo indeterminato
2. Gestione contratto a tempo determinato
3. Gestione contratto per supplenze brevi e saltuarie

Gestione contratto a tempo indeterminato.

Tale attività prevede il trattamento di tutti dati personali funzionali al perfezionamento dell'assunzione del personale docente a tempo indeterminato, con riferimento agli aspetti relativi al trattamento giuridico ed economico ed alla verifica del possesso dei requisiti per l'assunzione.

La suddetta attività comporta, nel trattamento dei dati personali, una contitolarità ex art. 26 del Reg. (UE) 2016/679 del Ministero e della scuola. Considerato che l'attività si svolge tramite funzioni SIDI, il responsabile esterno del trattamento è il fornitore del sistema informativo del Ministero.

Gestione contratto a tempo determinato

Questa attività prevede il trattamento di tutti i dati personali funzionali all'assunzione del personale docente a tempo determinato, con riferimento agli aspetti relativi al trattamento giuridico ed economico ed alla verifica del possesso dei requisiti per l'assunzione. Come nel caso del personale di ruolo, vi è una contitolarità ex art. 26 del Reg. (UE) 2016/679 del Ministero e dell'istituzione scolastica nel trattamento dei relativi dati personali. Considerato che l'attività si svolge tramite funzioni SIDI, il responsabile esterno del trattamento è il fornitore del sistema informativo del Ministero.

Gestione contratto per supplenze brevi e saltuarie

Tale attività prevede il trattamento di tutti i dati personali funzionali all'assunzione del personale docente per supplenze brevi e saltuarie, con riferimento agli aspetti relativi al trattamento giuridico ed economico ed alla verifica del possesso dei requisiti per l'assunzione. L'attività comporta la titolarità esclusiva della scuola nel trattamento dei relativi dati personali, mentre il Ministero si pone come responsabile esterno del trattamento, in quanto autorità pubblica che, attraverso l'applicativo del portale SIDI, tratta dati personali per conto del titolare del trattamento.

Come avviene la gestione della privacy in caso di utilizzo di foto e telecamere

Foto degli alunni

Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali oppure quelli espressamente previsti dalla normativa di settore. Per tali trattamenti non sono tenute a chiedere il consenso degli studenti o dei genitori. In tale ottica la pubblicazione di foto degli alunni sui siti istituzionali o sui social afferenti alla scuola può essere considerata lecita in quanto tra le attività istituzionali rientra anche la realizzazione di eventi quali teatri, festival letterari o scientifici, open day, attività di orientamento, progetti e attività scolastiche. La riproduzione dei dati deve però rispondere alla sola esigenza di documentazione dell'attività didattica, in ossequio al principio di proporzionalità. Per cui le riprese degli eventi dovrebbero essere limitate al gruppo nello svolgimento dell'attività, evitando i primi piani. Gli studenti devono essere sempre ripresi in atteggiamenti positivi o costruttivi, mai negativi. La diffusione delle immagini (su internet) deve essere, invece, soggetta al consenso dei genitori.

Telecamere a scuola

L'installazione di sistemi di videosorveglianza nelle scuole deve comunque garantire i diritti degli studenti. E' ammissibile nei casi in cui sia indispensabile, al fine di tutelare l'edificio e i beni scolastici da atti vandalici, restringendo le riprese alle sole aree interessate. Ovviamente la presenza delle telecamere va segnalata con appositi cartelli e, comunque, le telecamere all'interno della scuola vanno attivate solo dopo la chiusura degli orari scolastici e non in coincidenza delle attività scolastiche ed extrascolastiche. IL Consiglio d'Istituto ha disposto un regolamento in merito, scaricabile dalla pagina web della scuola.

Gestione del Rischio Data breach

MISURE DI ACCOUNTABILITY (RESPONSABILIZZAZIONE) DI TITOLARI E RESPONSABILI

Il Data breach è una violazione dei dati personali, causata, accidentalmente o in modo illecito, dalla distruzione, dalla perdita, dalla modifica, dall'accesso o dalla divulgazione non autorizzata dei dati personali conservati o trattati. Il Regolamento per la protezione dei dati personali pone con forza l'accento sulla "responsabilizzazione" (accountability) di titolari e responsabili – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento *(artt. 23-25, in particolare, e l'intero Capo IV del regolamento)*. Si tratta di una grande novità in tema di protezione dei dati, in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento. Il primo fra tali criteri è sintetizzato dall'espressione inglese "data protection by default and by design" *(art. 25)*, ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili per tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25(1) del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono attivare una serie di misure specifiche e dimostrabili. La stessa designazione di un "responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer) riflette l'approccio responsabilizzante che è proprio del regolamento *(si veda art. 39)*, essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare/del responsabile. Non è un caso, infatti, che

fra i compiti del RPD rientrino “la sensibilizzazione e la formazione del personale” e la sorveglianza sullo svolgimento della valutazione di impatto di cui all’art. 35.

Dunque, il titolare del trattamento ha due obblighi: tutela diritti degli interessati e la gestione del rischio di Data breach.

Fondamentale, fra tali attività, è la gestione del rischio inerente al trattamento. Quest’ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione *(artt. 35-36)* tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi (vedi le linee-guida in materia di valutazione di impatto sulla protezione dei dati adottate dal Gruppo “Articolo 29”, qui disponibili: www.garanteprivacy.it/regolamentoue/DPIA). All’esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l’autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l’autorità non ha il compito di “autorizzare” il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell’art. 58: dall’ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento. Dunque, l’intervento delle autorità di controllo sarà principalmente “ex post”, ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; infatti, a partire dal 25 maggio 2018 alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all’autorità di controllo e il cosiddetto *prior checking* (o verifica preliminare), sono stati sostituiti dagli obblighi di tenere un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia, con successiva eventuale consultazione dell’Autorità.

Nell’ambito della tutela e della gestione del rischio, si analizzano i principali adempimenti da parte del titolare e del responsabile del trattamento dei dati.

Aggiornamento delle informative privacy a scuola

La prima operazione da eseguire per l’adeguamento al GDPR (n°679/206, promulgato il 25 maggio 2018) è l’aggiornamento delle informative da comunicare agli interessati. E’ sufficiente pubblicare l’informativa sul sito web dell’istituto. Queste informative devono contenere informazioni relative al periodo di conservazione dei dati, la base giuridica, i diritti dell’interessato e tutti i requisiti previsti dagli art. 12, 13 e 14 in merito all’obbligo informativo. Fino al compimento del 18° anno di età, i minorenni non possono rilasciare consenso al trattamento dei dati. Compiuto il 18° anno di età, solamente il diretto interessato può rilasciare il consenso (né i genitori né chi aveva esercitato la potestà genitoriale). Il consenso non è obbligatorio per la fruizione di servizi per prevenzione e consulenza fornita direttamente ai minori, come lo sportello di ascolto e sostegno all’infanzia. Per trattamenti speciali dei dati, come foto, riprese, audio e video, e relativa diffusione, occorre l’esplicita autorizzazione degli interessati. Nella pubblica amministrazione, i tempi di conservazione dei dati personali raccolti sono stabiliti dal Ministero dei Beni e delle Attività Culturali.

Registro dei trattamenti

E’ un registro delle operazioni di trattamento i cui contenuti sono indicati all’art. 30. Si tratta di uno strumento fondamentale non soltanto ai fini dell’eventuale supervisione da parte del Garante, ma anche

allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante. Tenere questo registro è obbligatorio per tutte le imprese con almeno 250 dipendenti. Le aziende con meno di 250 dipendenti sono escluse da quest'obbligo se il trattamento dei dati non comporta un rischio per i diritti e le libertà degli interessati. Le scuole, trattando continuamente dati, soprattutto particolari, hanno l'obbligo di tenere questo registro: un documento scritto in formato elettronico, che deve essere continuamente aggiornato ed esibito durante l'eventuale controllo del Garante. Esso è utile anche come riepilogo completo dello stato attuale dei trattamenti per chi lo redige. Per ogni attività è opportuno specificare la base giuridica, le operazioni svolte sui dati, le modalità del trattamento, il tipo di informativa e l'eventuale presenza di responsabili esterni. Il registro deve contenere almeno:

- Nome e contatti del titolare, contitolare, rappresentante del trattamento e responsabile della protezione dei dati
- Finalità del trattamento
- Descrizione della categoria di interessati e di dati trattati
- Descrizione della categoria di destinatari dei dati, comprese terze parti
- Eventuali trasferimenti di dati
- Termini di cancellazione dei dati
- Misure di sicurezza (tecniche e organizzative)

Queste sono le informazioni minime da inserire nel registro, ma è consigliabile riportare ogni altra informazione utile a migliorare questa analisi dei trattamenti e dei relativi rischi.

Misure di sicurezza

Le misure di sicurezza devono garantire un livello di sicurezza adeguato al rischio del trattamento (art. 32, paragrafo 1); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso"). Per lo stesso motivo, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza *(ex art. 33 Codice)* poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento.

Prevenzione e gestione della valutazione d'impatto

Il principio di accountability, che ha aumentato le responsabilità del titolare del trattamento dei dati personali, chiamato ad adottare misure tecniche e organizzative di sicurezza per la protezione di dati personali, basate sui principi del "risk based". A scuola, i rischi di Data Breach possono essere legati ai seguenti fattori:

- Comportamenti errati (disattenzione, inconsapevolezza, condotte fraudolente, furto, smarrimento) del personale amministrativo scolastico, dei docenti, degli alunni o dei genitori.
- Violazione informatica (virus, malware, sabotaggio, intercettazioni, obsolescenza degrado, malfunzionamento) esterna e/o interna.
- Violazione contestuale (eventi imprevedibili naturali, dolosi, artificiali o accidentali) all'impianto scolastico.

Cosa fare in caso di Data breach a scuola

Il verificarsi del Data breach fa scattare al titolare tre adempimenti:

- Notifica di violazione al Garante per la protezione dei dati personali
- Eventuale comunicazione della violazione all'interessato
- Aggiornamento del registro delle violazioni con circostanze, conseguenze e provvedimenti adottati per porvi rimedio.

A partire dal 25 maggio 2018, tutti i titolari devono notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che tale violazione comporti dei rischi per i diritti e le libertà degli interessati. Pertanto, la notifica all'autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo".

Il titolare del trattamento dovrà in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati *(si veda art. 33, paragrafo 5). Pertanto, il* titolare del trattamento deve adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Comportamenti da attuare in caso di perdita o hackeraggio di dati sensibili

Nel caso il dipendente verifichi la perdita di dati sensibili, relativi a personale o alunni, tramite smarrimento o furto dei dati installati in una pendrive o hardisk esterno, lo stesso è tenuto a dare comunicazione scritta al Dirigente indicando le modalità di perdita dei dati e la natura dei dati stessi. Per dati sensibili si intendono quelli che rilevano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale.

Analoga comunicazione deve essere effettuata nel caso in cui il dipendente si accorga che dal device in uso siano stati hackerati i dati sensibili posseduti. Di conseguenza sarà compito del dipendente produrre copia della denuncia di smarrimento/furto inoltrata alla locale Tenenza dei Carabinieri.

Formazione, informazione per le diverse componenti scolastiche

All'inizio di ogni anno scolastico, il personale scolastico viene informato sui meccanismi di gestione dei dati in conformità con il profilo professionale. La formazione è svolta dal DPO.