



**Monthly Roundup | Mag '21**

## MONTHLY ROUNDUP

### Maggio 2021

I principali aggiornamenti in materia di TMT & Data Protection del mese di Maggio 2021

---

#### NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

- Standard contractual clauses for international transfers [[Link](#)]
  - Standard contractual clauses for controllers and processors in the EU/EEA [[Link](#)]
  - Final version of the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data [[Link](#)]
  - Garante privacy: no al controllo indiscriminato dei lavoratori - Ordinanza ingiunzione nei confronti di Comune di Bolzano del 13 maggio 2021 [[Link](#)]
- 

#### PRINCIPALI AGGIORNAMENTI



diritti d'autore e sia Facebook che Sisal per atti di concorrenza sleale parassitaria.

Per maggiori informazioni:

<https://bit.ly/3xaGaGA>

<https://bit.ly/3xkrGEt>

**Qual è la tutela giuridica offerta dalle app per dispositivi mobili, il cui ritmo di sviluppo è davvero vertiginoso?**

\*\*\*

Ne abbiamo parlato su RiskManagement360, analizzando due pronunce della Sezione specializzata in materia di impresa del Tribunale di Milano (caso Business Competence vs Facebook e caso Satispay vs Sisal), in cui i giudici hanno condannato Facebook per violazione dei

SEGUE →



### **Garante privacy: no al controllo indiscriminato dei lavoratori**

Non è possibile monitorare la navigazione internet dei lavoratori in modo indiscriminato. Indipendentemente da specifici accordi sindacali, le eventuali attività di controllo devono comunque essere sempre svolte nel rispetto dello Statuto dei lavoratori e della normativa vigente in materia di privacy e protezione dei dati personali. È quanto affermato dal Garante Privacy in un provvedimento sanzionatorio emesso nei confronti del Comune di Bolzano (**“Comune”**), a conclusione di un’istruttoria avviata sulla base del reclamo presentato da un dipendente che, nel corso di un procedimento disciplinare, aveva scoperto di essere stato costantemente controllato (**“Provvedimento”**).

L’amministrazione, la quale inizialmente aveva contestato al proprio dipendente la consultazione di *Facebook* e *YouTube* durante l’orario di lavoro, aveva poi archiviato il procedimento per l’inattendibilità dei dati di navigazione raccolti.

Dagli accertamenti del Garante Privacy è emerso che il Comune impiegava, da circa dieci anni, un sistema di controllo e filtraggio della navigazione in internet dei propri dipendenti, con la conservazione dei dati per un mese e la creazione di apposita reportistica, per finalità di sicurezza della rete. Sebbene il datore di lavoro avesse stipulato un accordo con le organizzazioni sindacali, come richiesto dalla disciplina di settore, il Garante Privacy ha evidenziato che tale trattamento di dati deve comunque rispettare

anche i principi di protezione previsti dal Regolamento UE 2016/679 (**“GDPR”**).

Il sistema implementato dal Comune, senza aver adeguatamente informato i dipendenti, consentiva invece operazioni di trattamento non necessarie e sproporzionate rispetto alla finalità di protezione e sicurezza della rete interna, effettuando una raccolta preventiva e generalizzata di dati relativi alle connessioni ai siti web visitati dai singoli dipendenti.

Il sistema raccoglieva inoltre anche informazioni estranee all’attività professionale e comunque riconducibili alla vita privata dell’interessato.

Con il Provvedimento emesso, il Garante Privacy ha ricordato che l’esigenza di ridurre il rischio di usi impropri della navigazione in Internet non può condurre al completo annullamento di ogni aspettativa di riservatezza dell’interessato sul luogo di lavoro, anche nei casi in cui il dipendente utilizzi i servizi di rete messi a disposizione dal datore di lavoro.

Nell’ambito dell’istruttoria sono state inoltre riscontrate violazioni anche in merito al trattamento di dati relativi alle richieste di accertamento medico straordinario da parte dei dipendenti, effettuate attraverso un apposito modulo. Quest’ultimo, messo a disposizione dall’amministrazione, prevedeva la presa visione obbligatoria da parte del dirigente dell’unità organizzativa, circostanza che comportava un trattamento illecito di dati relativi allo stato di salute.

Il Garante Privacy, tenendo conto della piena collaborazione dell’amministrazione, ha disposto una sanzione di Euro 84 mila per l’illecito trattamento dei dati del personale.

In aggiunta alla sanzione pecuniaria, il Comune dovrà altresì adottare misure tecniche e organizzative per anonimizzare il dato relativo

alla postazione di lavoro dei dipendenti, cancellare i dati personali presenti nei log di navigazione web registrati, nonché aggiornare le procedure interne individuate e descritte nell'accordo sindacale.

\* \* \*



### The European Commission adopts new tools for safe transfers of personal data

Pursuant to Article 46(1) lett. c) of the General Data Protection Regulation no. 2016/679 ("**GDPR**"), the European Commission ("**EC**") may adopt standard contractual clauses ("**SCCs**") which provide appropriate safeguards for the transfer of personal data to a third country or an international organisation in compliance with the GDPR requirements.

Considering the above, on 4 June 2021, the EC adopted a set of **SCCs for the transfer of personal data to third countries**.

The aforementioned sets of SCCs have been adopted in order to:

- implement new requirements under the GDPR;
- take into account the Schrems II judgement of the European Court of Justice ("**ECJ**"), aimed at ensuring a high level of data protection for citizens.

In particular, on 16 July 2020, through the Schrems II judgement, the ECJ confirmed the

validity of the EU SCCs for transfers of personal data to a third country or an international organisation, while invalidating the EU-US Privacy Shield. Thus, the ECJ ruled that international data flows under the European Union's comprehensive data protection regime, can continue to be based on EU SCCs, while also clarifying the conditions under which they can be used.

But let's proceed with order.

### What are the SCCs?

Pursuant to Article 46(1) of the GDPR, "*in the absence of an adequacy decision of the European Commission, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available*".

According to the GDPR, among the measures that represent adequate safeguards and, therefore, can be used as a ground for data transfers from the EU to third countries, SCCs adopted by the EC can be included.

In particular, the SCCs are standardised model data protection clauses, pre-approved by the EC, which can be incorporated into contractual arrangements on a voluntary basis, providing an easy-to-implement tool to comply with data protection requirements.

### The new SCCs approved by the EC

As clarified by the EC, the new SCCs, adopted due to the new requirements introduced by the GDPR and taking into account the Schrems II judgement of the ECJ, will replace the three sets of SCCs which were adopted under the previous Data Protection Directive 95/46.

SEGUE →

The new SCCs, which have been adopted after having taken into account the joint opinion of the European Data Protection Board ("EDPB") and the European Data Protection Supervisor ("EDPS"), as well as the Member State's opinion and stakeholders' feedback received during a broad public consultation, introduce the following main innovations:

an update in order to align them to the provisions of the GDPR;  
one single entry-point covering a broad range of transfer scenarios (e.g., data transfer (i) from controller to controller; (ii) from controller to processor; (iii) from processor to processor; and (iv) from processor to controller), instead of separate sets of clauses;  
more flexibility for complex processing chains, through a 'modular approach' and by offering the possibility for more than two parties to adhere and use the clauses;  
practical toolbox to comply with the Schrems II judgment (i.e. an overview of the different steps that companies have to take in order to comply with the Schrems II judgment as well as examples of possible 'supplementary measures', such as encryption, that companies may implement, if necessary).

Moreover, as clarified by the EC, for controllers and processors which are currently using previous sets of standard contractual clauses, a transitional period of 18 months is provided.

## Conclusions

As declared by the EC, the new SCCs will offer more legal predictability to businesses and help small-medium enterprises, in particular throughout the easy-to-implement template, to ensure compliance with requirements for safe data transfers, while allowing data to move freely across borders, without legal barriers.

Moreover, since these SCCs have been issued in a moment in which a large number of regional organisations and third countries are developing or have already adopted their own standard contractual clauses on the basis of converging principles, the EC has committed itself to intensify its cooperation with such international partners in order to further facilitate data transfers between different areas of the world.

\* \* \*

Per maggiori informazioni, potete contattare:

**Carlo Impalà**  
*Partner e Responsabile Dip. TMT e Data Protection*  
*(Carlo.Impala@MorriRossetti.it)*



**Morri Rossetti**



**Osservatorio TMT&DP**





**Morri Rossetti  
Piazza Eleonora Duse, 2  
20122 Milano**

**MorriRossetti.it  
Osservatorio-dataprotection.it**