

THE PROTECTION OF PERSONAL DATA IN CREDIT INFORMATION SHARING

ALESSANDRA PIERUCCI *ITALIAN DATA PROTECTION AUTHORITY*



WORLD BANK GROUP

IFC | International
Finance Corporation



Summary

Italian Data Protection Authority – Garante per la protezione dei dati personali

Data processing at ‘credit information systems’(Credit Bureaux)

Bank of Italy’s Central Credit Register

Bank Alert System

(Private) Credit Information Systems (SIC) (CRAs – Credit Bureaux)

Key Principles in the Code of Conduct on personal data processing by Credit Bureaux

Data Retention Periods

Work in Progress: The Revised Code of Conduct

Codes of conduct in the new EU General Data Protection Regulation

Italian Data Protection Authority – Garante per la protezione dei dati personali

COMPOSITION: 4 Commissioners, elected by Parliament (7-year term); Office: Secretary General + Staff (125)

TASKS (as set up by Legislative Decree no. 196/2003, so called ‘DPCode’)

- Enforcing data protection law
- Handling of complaints (quasi-judicial procedure)
- Decisions on cases, Guidelines, Recommendations
- Inspections (on-the-spot, desk) + investigations
- Prior authorisations (general for sensitive data, ad-hoc)
- Administrative fines
- Fostering knowledge and awareness of data protection law
- Media (website, newsletters, info campaigns)
- Parliament, civil society, EU bodies and institutions
- Cooperation with other DPAs (Article 29 WP plus other forums: Council of Europe, OECD, IDPC)
- Meetings, workshops

website: www.garanteprivacy.it

Data processing at 'credit information systems' (credit bureaux)

Credit bureaux in Italy

Public

Bank of Italy's
Central Credit
Register

Bank of Italy's
Alert System

Private

'Credit
Information
Systems'

Bank of Italy's Central Credit Register

Features:

- A 'public database run by Bank of Italy;
- It ensures stability in the credit sector vis-à-vis the increase in loan applications and prevents repeated overindebtedness and/or contractual non performance

Recorded information:

- Loans of or above Euro 30,000 plus 'bad' debt regardless of the amount

(continued) Bank of Italy's Central Credit Register

Key processing principles applying to CCR personal data:

- **No information notice**, as the data were collected from third parties pursuant to a legal obligation (Sec. 13(4) DP Code);
- **No consent by data subjects**, as the processing is regulated by the specific provisions applying to public bodies whereby no consent is needed when public bodies discharge the tasks entrusted to them by law in line with the relevant laws and regulations (Sec. 24(1)(a) DP Code);
- **No exercise of data subjects' rights**, as the processing concerns data collected 'for purposes exclusively related to currency and financial policy, the system of payments, control of brokers and credit and financial markets and protection of market stability' (Sec. 8(2)(d) DP Code and Article 13(1)(e) Directive 95/46/EC).

Bank Alert System

Features:

- **A 'public' database** run by Bank of Italy (data controller) whose technical management is committed to SIA, a company appointed as data processor;
- **Regulated by specific provisions** (Law No. 386 of 15 December 1990; Law No. 205 of 25 June 1999; legislative decree No. 507 of 30 December 1999; Sect. 13 of Bank of Italy's Regulations dated 29 January 2002 - 'Operation of the computerised register for bank and postal cheques and payment instruments'). It includes information on:
 - **Measures or reports** concerning individuals that have issued bounced or uncleared cheques, holders of revoked credit/debit cards (because of defaults) or cheques or credit/debit cards that have been stolen, lost or blocked.

Key principles applying to the processing of personal data:

- Data subjects are entitled to exercise the rights set forth in Sec. 7 of the DP Code vis-à-vis the reporting entities.

(Private) 'Credit Information Systems' (SIC) (CRAs – Credit Bureaux)

- **'Private' databases** run by private entities, which determine their terms of use and operation;
- **Regulated by the 'Code of conduct for information systems run by private entities concerning consumer credit, reliability and timeliness in payments'** which has been in force since 2005;
- **'Participating entities'**: banks, financial intermediaries, other private entities that grant, as part of their commercial or professional activities, payment extensions for the supply of goods or services;
- **New participating entities: Additional entities** were allowed to access credit reports in SIC, in particular insurance companies and providers of (tele)communications services, pursuant to Sec. 6-a of decree No. 138 of 13 August 2011;
- **They record 'positive and negative information'** relating to all loan applications or credit histories

Key Principles in the Code of Conduct on personal data processing by Credit Bureaux

- **SPECIAL LEGAL VALUE OF THE CODE OF CONDUCT (Sec. 12 of the DP Code)**
- **Data processing safeguards and arrangements** are laid down in connection with the purposes of protecting credit and risk containment, in particular to assess data subjects' financial status and creditworthiness; no further purposes may be sought, such as market surveys or promotional initiatives;
- Ad-hoc forms must be used containing **specific information notices**; the information provided to each data subject by the participating entity must be supplemented by a more detailed notice under the SIC's own responsibility, possibly using electronic/computerised tools;
- **Customers must be informed suitably in advance of their inclusion** in the database;
- **Data retention periods** vary with the type of reported information (Section 6(2) of the Code of Conduct)

Data Retention Periods

NEGATIVE INFORMATION

12 months if default (up to 2 instalments) was remedied

24 months if default (over 2 instalments) was remedied

36 months if defaults were not remedied

(from contract expiry date, or from the date when the information was last updated)

POSITIVE INFORMATION

**36 months from contract expiry date/from
termination of credit history**

Work in Progress: The Revised Code of Conduct

- Reconsider **the scope of the Code** in the light of the developments in banking and financial instruments;
- **Simplify information** notices to take account of technological innovations;
- Reconsider the mechanisms for the so-called **prior notice of reporting** (to a credit bureau) to do away with ambiguities and the resulting litigations;
- Regulate the so-called '**new participating entities**' (under Sec. 6-a of decree No. 138/2011);
- Revise the provisions **on updating of the credit history** following e.g. transfer of debt (who is required to notify the CB of a remedied default if the bank transfers its debt to a debt collection company?);
- Reconsider the provisions on the **running of time for storage** of the data on non-remedied defaults: when does the 36-month term start? ('from the date the contract expires or the data was last updated'). The start date is calculated differently by the individual CBs .

Codes of conduct in the new EU General Data Protection Regulation

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

Article 40: 'The Member States, the supervisory authorities, the Board and the Commission shall **encourage the drawing up of codes of conduct** intended to contribute to the proper application of the Regulation including:

(...) **out-of-court proceedings and other dispute resolution procedures** for resolving disputes between controllers and data subjects with regard to processing

The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it have **general validity within the Union**.

**THANK YOU FOR YOUR
ATTENTION!**

a.pierucci@gpdp.it

