Courtesy translation

French Data Protection Authority – CNIL

DECISION No.2023-144 of 21 DECEMBER 2023 APPROVING CONTROLLER BINDING CORPORATE RULES OF THALES
(application for approval No. 20005721)

The « Commission nationale de l'informatique et des libertés » (hereafter "CNIL"),

Pursuant to the request by THALES S.A. on behalf of the group THALES (hereafter "THALES"), for approval of their binding corporate rules for controller;

Having regard to Articles 47, 57 and 64 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation or GDPR);

Having regard to the CJEU decision *Data Protection Commissioner v. Maximillian Schrems and Facebook Ireland Ltd*, C-311/18 of 16 July 2020;

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021;

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023;

Having regard also to the French Data Protection Act 78-17 of 6 January 1978;

On a proposal from Ms. Anne DEBET, Commissioner, and the observations made by Mr. Damien MILIC, Government Commissioner;

Make the following observations:

1. Article 47(1) of the EU General Data Protection Regulation 2016/679 (GDPR), provides that the French Data Protection Authority (CNIL) shall approve Binding Corporate Rules (BCRs) provided that they meet the requirements set out under this Article.

2. The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees to controllers and processors established in the European Union ("EU") as to the protection of personal data that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country.

3. Before carrying out any transfer of personal data on the basis of the BCRs to one of the members of the group, it is the responsibility of any data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country of destination in the case of the specific data transfer, including onward transfer situations. This assessment has to be conducted in order to determine whether any legislation or practices of the third country applicable to the

to-be-transferred data may impinge on the data importer's and/or the data exporter's ability to comply with their commitments taken in the BCR, taking into account the circumstances surrounding the transfer. In case of such possible impingement, the data exporter in a Member State, if needed with the help of the data importer, should assess whether it can provide supplementary measures in order to exclude such impingement and therefore to nevertheless ensure, for the envisaged transfer at hand, an essentially equivalent level of protection as provided in the EU. Deploying such supplementary measures is the responsibility of the data exporter and remains its responsibility even after approval of the BCRs by the competent Supervisory Authority and as such, they are not assessed by the competent Supervisory Authority as part of the approval process of the BCRs.

4. In any case, where the data exporter in a Member State is not able to implement supplementary measures necessary to ensure an essentially equivalent level of protection as provided in the EU, personal data cannot be lawfully transferred to a third country under these BCRs. Therefore, the data exporter commits to waive, suspend or end the transfer of personal data. In the same vein, where the data exporter is made aware of any changes in the relevant third country legislation that undermine the level of data protection required by EU law, the data exporter is required to suspend or end the transfer of personal data at stake to the concerned third countries.

5. In accordance with the cooperation procedure as set out in the Working Document WP263 rev01[1], the Controller BCRs application of the group was reviewed by the CNIL, as the competent supervisory authority for the BCRs (BCR Lead) and by two Supervisory Authorities (SA) acting as co-reviewers. The application was also reviewed by the concerned SAs to which the BCRs were communicated as part of the cooperation procedure.

6. The review concluded that the Controller BCRs of the group comply with the requirements set out by Article 47(1) of the GDPR as well as the Working Document WP256 rev.01[2] and in particular that the aforementioned BCRs:

    i) Are legally binding and contain a clear duty for each participating member of the Group including their employees to respect the BCRs by entering in an Intra-Group Agreement (article 3 of the BCRs, appendix 12 of the BCRs and article 2 of the intra-group agreement);

    ii) Expressly confer enforceable third-party beneficiary rights to data subjects with regard to the processing of their personal data as part of the BCRs (article 10.2 of the BCRs);

    iii) Fulfil the requirements laid down in Article 47(2) of the GDPR:

[1] Endorsed by the EDPB on 25 May 2018.

[2] The WP256 rev.01 and WP264 are superseded by the EDPB Recommendations 1/2022. However, since the BCR-C of the group had already reached the stage of a "consolidated draft" in accordance with 2.4 of WP 263 rev.01 at the time of publication of the Recommendations, it can be assessed under the previous framework, subject to the EDPB adopting its opinion by the end of 2023 (paragraph 13 of the Recommendations).

a) The structure and contact details of the group of undertakings and each of its members are described in the Application form WP264 that was provided as part of the file review and appendix 8 of the BCRs;

b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question are specified in appendices 1 and 9 of the BCRs;

c) the legally binding nature, both internally and externally, of the Controller BCRs is recognized in article 3 of the BCRs, appendix 12 of the BCRs and article 2 of the intra-group agreement;

d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules are detailed in articles 4, 5, 8 and 13 of the BCRs;

e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22 of the GDPR, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Articles 77 and 79 of the GDPR, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules are set forth in articles 9, 10, 11 and 12 of the BCRs;

f) the acceptance by the controller or processor established on the territory of a Member State of its liability for any breaches of the binding corporate rules by any member concerned not established in the Union as well as the exemption from that liability, in whole or in part, only if the concerned party proves that that member is not responsible for the event giving rise to the damage are specified in article 9 of the BCRs;

g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of Article 47.2 of the GDPR are provided to the data subjects in addition to Articles 13 and 14 of the GDPR, is specified in article 17.1 of the BCRs;

h) the tasks of any data protection officer designated in accordance with Article 37 of the GDPR or any other person or entity in charge of monitoring the compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling are detailed in article 20 of the BCRs and in appendices 2, 3, 5, 6 and 7 of the BCRs;

i) the complaint procedures are specified in articles 11 and 12 of the BCRs and in appendices 2 and 3 of the BCRs;

j) the mechanisms put in place within the group of undertakings for ensuring the monitoring of compliance with the binding corporate rules are detailed in article 19 of the BCRs and appendix 5 of the BCRs. Such mechanisms include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. The results of such monitoring are communicated to the person or the entity referred to in point (h) above and to the board of the controlling undertaking of the group of undertakings and are available upon request to the competent supervisory authority;

k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authorities are specified in article 21 of the BCRs;

l) the cooperation mechanism put in place with the supervisory authority to ensure compliance by any member of the group of undertakings is specified in article 16 of the BCRs. The obligation to make available to the supervisory authority the results of the monitoring of the measures referred to in point (j) above is specified in article 19 of the BCRs;

m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules are described in article 8 of the BCRs;

n) finally, article 18 of the BCRs and appendix 6 of the BCRs provide for appropriate data protection training to personnel having permanent or regular access to personal data .

The EDPB issued opinion No 31/2023 on 28 November 2023 in accordance with Article 64(1) (f) of the GDPR. The CNIL took utmost account of this opinion.

Decides as following:

7. The CNIL approves the Controller BCRs of THALES as providing appropriate safeguards for the transfer of personal data in accordance with Article 46(1) and (2) (b) and Article 47(1) and (2) GDPR. For the avoidance of doubt, the CNIL recalls that the approval of BCRs does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which, an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

8. The approved BCRs will not require any specific authorization from the concerned SAs.

9. The Controller BCR of THALES must be brought in line with the EDPB Recommendations 1/2022 in the framework of the 2024 annual update.

10. In accordance with Article 58(2)(j) GDPR, each concerned SA maintains the power to order the suspension of data flows to a recipient in a third country or to an international organization whenever the appropriate safeguards envisaged by the Controller BCRs of THALES are not respected.

The President

Marie-Laure Denis

This decision may be subject to appeal before the Conseil d'État within a period of two months from the date of its notification.

Courtesy translation

ANNEX TO THE DECISION

The Controller BCRs of THALES that are hereby approved cover the following:

a. Scope. The BCRs apply when a BCR member is acting as a data controller or as in internal data processor (article 2.2 of the BCRs). The BCRs cover transfers of personal data from BCR members within the EEA to BCR members located outside the EEA, as well as to their onward transfers to other BCR members outside the EEA (article 2.3 of the BCRs).

b. EEA countries from which transfers are to be made: France, Austria, Belgium, Denmark, Estonia, Finland, Germany, Greece, Hungary, Italy, Latvia, Netherlands, Norway, Poland, Portugal, Romania, Spain and Sweden (appendix 8.1 of the BCRs).

c. Third countries to which transfers are to be made: Algeria, Argentina, Australia, Bahrain, Bolivia, Brazil, Cameroun, Canada, Chile, China, Colombia, Egypt, Gabon, Hong-Kong, India, Indonesia, Israel, Ivory Coast, Japan, Kazakhstan, Kenya, Lebanon, Malaysia, Mauritius, Mexico, Morocco, New Zealand, Nigeria, Oman, Pakistan, Philippines, Qatar, Saudi Arabia, Senegal, Singapore, South Africa, South Korea, Switzerland, Taiwan, Thailand, Turkey, United Arab Emirates, United Kingdom, United States of America and Venezuela (appendices 8.2 and 9 of the BCRs).

d. Purposes of the transfer: The purposes are detailed in appendix 1 of the BCRs, as follows:

01 Management of the Information System and phone network, control of access to the Information System as well as to various IS/IT tools (software, applications, printers, etc.), management of authorizations and of the appointments of IS/IT administrators related thereto, user authentication and management of their profiles, monitoring of the actions they carry out (e.g., modification of database)

02 Implementation of an e-mailing system

03 Monitoring and auditing connections to certain IT tools and databases in order to determine the use rate and calculate the cost of related licenses, analysis of websites browsing by users to understand their use and improve the concerned website(s)

04 Implementation of IS/IT security audits, management and monitoring of security breaches/incidents, implementation of procedures for data back-up and business continuity in the event of incidents impacting the Information System

05 Management and follow-up of IS/IT assistance requests submitted by users to the Helpdesk

06 Management of phones and associated phone networks available to employees

07 Management of collaborative tools

08 Follow-up of employees on business trip to ensure their security

09 Recruitment of employees and follow-up of applications

10 Workforce administration, employees profiles, management of organizations, reporting and data analytics

11 Management of:
- performance, remuneration, financial or non-financial benefits
- career and skills development

12 Management of pay, administrative file of employees (presence, absence, sick leave, retirement, transfers, etc.) and work-time follow-up

13 Management of professional training

14 Management of employee on international assignment (follow-up of their mission, support measures, family situation)

15 Management of travels, booking and payment of travel documents, as well as reimbursement to employees of travel expenses, follow-up and management of expenses submitted by employees, gifts and hospitality that employees may consider accepting or offering and of professional credit cards

16 Implementation of corporate network, including social corporate network

17 Management of the workload, organization and monitoring of projects and activity

18 Management of employee surveys

19 Management of the employment policy of disabled workers

20 Follow-up of inventions notifications in the context of activities relating to intellectual property

21 Creation and management of insiders list as well as management of anti-corruption declaration, due diligence procedure in relation to partners, the management of the whistle-blowing, internal investigation and conflicts of interests procedures

22 Monitoring compliance in terms of trade compliance

23 Management of administrators including in order to comply with the legal obligations

24 Document management

25 Management of employees' feedbacks and of their satisfaction, follow-up of suggestions submitted by them (e.g., suggestion box)

26 Management of employees and providers clearances for the purpose of obtaining the accreditations and/or clearances necessary (i) to validate the conformity of data, documents, products or services with norms, standards or regulations or (ii) to carry out verifications or audits

27 Management, follow-up and inventory of the real estate portfolio of the group

28 Management and follow-up of employees' claims or solicitations for indemnity, management of the relationships with insurers in this respect

29 Study and resolution of third-party claims, solicitations for indemnity, litigation and pre-litigation, and for the determination of counsel assisting Thales in litigation and pre-litigation procedures

30 Processing for events organization and communication purposes

31 Relationship management with customers, partners and prospects

32 Management of mergers and acquisitions operations

33 Management of the relationships with the suppliers and subcontractors, involving in particular the management of the purchases and the monitoring of the contractual relationships

34 Management of booking, purchase, evaluation and provision of training by Thales for the benefit of its internal and/or external clients

35 Submission of applications in the context of calls for tenders initiated by potential customers, involving in some cases exchanges of data with bidding partners

36 Follow-up and management of the use of interactive platforms and networks made available to end customers and of purchases made by the latter on the said interactive platforms and networks

37 Processing for the purpose of adapting and setting up products in accordance with the customers' needs

38 Managing incidents on trains and incident reports made by THALES employees

39 Data processing intended to ensure the organization, follow-up and performance of training sessions provided by THALES for its customers

40 Data processing resulting from technical support and maintenance operations carried out for Thales customers

41 Processing for participating in and/or implementing research projects

42 Processing for obtaining grants

43 Personal data collection and processing for regulatory and economic watch as well as strategic intelligence

44 Accounting and tax management as well as controlling financial operations

45 Implementation of internal audits within the group and follow-up of the actions resulting therefrom

e. Categories of data subjects concerned by the transfer: Those categories are specified in article 2.2 of the BCRs and appendix 1 of the BCRs, as follows:

- THALES' employees, including THALES' salaried employees, representatives and officers, as well as THALES' former employees;
- THALES' temporary workers and interns;
- THALES' job applicants;
- employees and contact points of THALES' clients and prospects;
- employees and contact points of THALES' partners, providers, suppliers and subcontractors;
- users of application and public data subjects;
- employees, contact points and clients of internal clients (internal client means any THALES entity acting as data controller, for which another THALES entity processes personal data in the frame of a contract for the provision of services or products implying personal data processing).

f. Categories of personal data transferred: Those categories are included in article 2.2 of the BCRs and are specified in appendix 1 of the BCRs, as follows:

- identification data;
- data related to professional life;
- connection data;
- biometric data;
- data related to personal life;
- economic and financial data;
- sensitive personal data (i.e., data related to health);
- location data;
- driving license;
- any publicly available information; and
- data related to the use of interactive services.