Deliberation 2018-303 of September 6, 2018 National Commission for Computing and Liberties Nature of the deliberation: Recommendation Legal status: In force Date of publication on Légifrance: Wednesday October 10, 2018 Deliberation No. 2018-303 of September 06, 2018 adopting a recommendation concerning the processing of data relating to the payment card for the sale of goods or the provision of services remotely and repealing deliberation no. 2017-222 of July 20, 2017 The National Commission for Data Processing and Freedoms, Having regard No. 108 of the Council of Europe for the protection of individuals with regard to the automatic processing of personal data; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 relating to 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 regulation on data protection - GDPR); Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; Having regard to the Civil Code; Having regard to the Consumer Code; Having regard to the Monetary and Financial Code; Having regard to Law No. 78-17 of 6 January 1978 as amended relating to data processing, files and freedoms; Having regard to Decree No. 2005- 1309 of October 20, 2005 amended taken for the application of law n ° 78-17 of January 6, 1978 relating to data processing, files and freedoms; Having regard to the deliberation of the National Commission for Data Processing and Freedoms n ° 2005-213 of October 11, 2005 adopting a recommendation concerning the methods of electronic archiving, in the private sector, of personal data; Having regard to the guidelines concerning the impact analysis relating to data protection (AIPD) and the manner of det Determine whether the processing is likely to create a high risk for the purposes of Regulation (EU) 2016/679 adopted on 4 October 2017 by the Article 29 Data Protection Working Party; Having regard to Recommendation No R (90) 19 of the Council of Europe on the protection of personal data for payment purposes and other related operations; Considering the recommendations of the European Central Bank for the security of online payments published on January 31, 2013; After having heard Mr François PELLEGRINI, Commissioner, in his report, and Mrs Nacima BELKACEM, Government Commissioner, in her observations, Makes the following observations: storage and use of the bank card number in the distance selling sector.Ten years after the adoption of this recommendation, the Commission adopted a new deliberation aimed at updating assess and propose concrete recommendations for the use of the bank card number by distance selling professionals in automated processing. It now considers it necessary to update its recommendation with regard to the evolution of trade practices online, as well as that of the legal and technological framework. The provisions of this

recommendation, which repeals that of 2017, apply to the processing of data relating to the payment card (interbank card or similar device), hereinafter the card, during any sale of goods or provision of a service concluded, without the simultaneous physical presence of the parties, between a consumer (natural person) and a professional, and which, for the conclusion of this contract, exclusively use one or more remote communication techniques (Internet, telephone, etc.). The payment cards referred to are those which notably enable purchases to be made from a merchant or a service provider affiliated with a national or international payment network (CB system, Visa, MasterCard, etc.) but also so-called payment cards private (cards issued by merchants or by financial institutions specializing in consumer credit) and credit (card presented by a member to a supplier affiliated with the card issuer's network). The Commission clarifies that Article 35 of the GDPR provides for the conduct of a data protection impact assessment (DPIA), when the processing of personal data is likely to create a high risk for the rights and freedoms of the persons concerned, taking into account in particular the nature of the data processed. In this respect, the Commission recalls that financial data, including data relating to payment cards, are qualified as highly personal data given the seriousness of the impacts for the persons concerned that their violation could cause (use for payments fraudulent for example). The Commission reminds organizations that would implement such processing of payment data that they are likely to be required, depending on the extent of the processing and the methods of its implementation, to carry out a DPIA.Article 1: Purposes of processingThe protection of personal data, and thereby of privacy, implies the ability of the individual to control the collection, recording and use of the personal data that he is required to communicate in the context of of a payment. The primary purpose of using a payment card number is to enable a transaction to be carried out aimed at the delivery of goods or the provision of a service in return for full payment. a price. The collection of data relating to a payment card can however fulfill other purposes, linked to the particularity of remote operations: the reservation of goods or services; the payment of subscriptions taken out in im line plicating defined and regular payments; the simplification of any subsequent purchases on the merchant's site; the offer of payment solutions dedicated to distance selling by payment service providers (virtual cards, digital card holders known as wallets, rechargeable accounts, etc.). These solutions aim to prevent consumers from having to enter data relating to their card during purchases made remotely; the fight against fraud. The Commission considers that these purposes are determined, explicit and legitimate. It recalls that the data collected and processed for the purpose of settling multiple and regular payments within the framework of subscriptions cannot subsequently be used for another purpose such as, for example, facilitating subsequent one-off payments, and vice versa. In addition, given the

sensitivity of this data , the payment card number cannot be used as a commercial identifier. Article 2: Legal basis for processing The Commission considers that the legal basis for processing bank data may vary depending on the purpose pursued, the nature of the transaction concluded and the methods of its execution, in accordance with Article 6 of the GDPR. The Commission recalls that it is the responsibility of the person responsible of processing to ensure the conditions of lawfulness of its processing and, in particular, the legal basis on which to base it.Single paymentThe Commission notes that the bank card number can only be collected and processed to enable the performance of a transaction in the context of the performance of the contract concluded by the data subject in accordance with Article 6-1-b of the GDPR (contractual performance). Thus, in the event of a contract involving a single payment, the Commission considers that the data are therefore not intended to be kept beyond the time of the commercial transaction.Subscription involving multiple paymentsThe Commission considers that in the context of a subscription contract taken out online involving, in fact, successive and regular payments, the retention of bank data also satisfies the condition provided for in Article 6-1-b of the GDPR (contractual performance). Payment solutions dedicated to distance sellingAs regards the processing of bank data in connection with the subscription to a payment solution dedicated to distance selling by payment service providers (virtual cards, card holders digital – wallets, rechargeable accounts, etc.), the Commission considers that the communication of bank details also falls within the framework of the performance of the contract, the latter specifically aimed at keeping the data relating to the payment card in order to avoid consumers having to enter them when making purchases at a distance.The option to facilitate any subsequent paymentsThe Commission considers that keeping the customer's card number in order to facilitate any subsequent payments, and possibly being able to make a purchase in one click on the merchant's site, goes beyond the execution of the contract concluded. It retains that this option constitutes an option independent of the initial act that led to the collection of bank details and recalls that such processing requires that the free, specific, informed and unequivocal consent of the persons be obtained beforehand, pursuant to Article 6-1-a of the GDPR. The subscription to a subscription, free of charge or against payment, giving access to additional services, reflecting the customer's registration in a regular commercial relationship The Commission recalls that the retention of the customer's card number in order to facilitate its possible subsequent payments on the merchant's site goes beyond the execution of the contract concluded. The Commission considers, however, that the fact for a person to take out a subscription which gives access to additional services to those accessible to any customer may reflect the customer's intention to enter into a regular business relationship. These additional

services may take the form of additional ancillary services requested by the customer (fast delivery, access to private sales or additional content, etc.). In such cases, the Commission considers that the retention of the person's bank details to facilitate subsequent purchases may be based on the legitimate interest of the data controller, the person being able, under their conditions, to reasonably expect that his bank details are kept to simplify his subsequent purchases. The Commission specifies that the customer's intention to enter into a regular commercial relationship must be manifest. The subscription to such a subscription must therefore be distinct from the simple creation of a customer account giving access to the basic services. This must be a complementary process to the creation and day-to-day operation of a customer account. Subscription to the subscription may nevertheless take place at the same time as the creation of a customer account. Similarly, the Commission considers that the simple registration in a program or loyalty account, in return for advantages and rewards, which does not would not give access to additional services aimed at facilitating purchases, cannot sufficiently reflect the customer's intention to make regular purchases from the merchant, thus justifying the retention of his bank details by default, on the basis of interest legitimate interest of the data controller. In addition, in order to be able to rely on the basis of the legitimate interest to carry out such processing, the data controller must clearly inform the persons concerned and allow them to oppose it by making include a mention and a visible, explicit and ergonomic means such as a checkbox, directly on the collection medium (see article 5 of this deliberation port ant on information and the rights of individuals). The fight against payment card fraudThe Commission considers that the retention of payment card data beyond the completion of a transaction for the purposes of the fight against payment card fraud does not fall within the framework of the contract. It considers that this processing is in the legitimate interest of the data controller, subject to not disregarding the interests or rights and freedoms of individuals pursuant to Article 6-1-f of the GDPR, by guaranteeing in particular compliance with the principles of transparency and the effective exercise of their rights by the persons concerned. The Commission points out that the use of the bank card number in the context of processing aimed at combating fraud and, if necessary, the keeping of a trace of fraudulent behavior having generated unpaid bills cannot lead to a refusal of sale. The Commission specifies that this use may nevertheless lead the merchant to refuse this method of payment.Article 3: Data collectedThe data necessary to carry out a remote transaction by payment card are the card number, the date of expiration and the visual cryptogram. The Commission recalls that only adequate, relevant data limited to what is necessary with regard to the purpose of the processing must be collected. With regard to the identity of the card holder, when this data is not required for carrying out an online transaction, it must not be

collected by the payment system except when it is justified for the pursuit of a specific and legitimate purpose, such as the fight against fraud. The Commission also considers that the data controller, or its service provider, cannot request the transmission of the photocopy or digital copy of the front and/or back of the payment card, even if the visual cryptogram and some of the numbers are hidden. Indeed, the transmission of this document is not compatible with the security obligations and the conditions of use that the holder of the payment card must respect in accordance with article L. 133-16 of the monetary and financial code. Article 4: On the retention period of the data The Commission recalls that pursuant to Article 5-1-e of the GDPR, the data must be kept for a period not exceeding that necessary with regard to the purposes for which they are processed. It recalls in this respect that the retention of the cryptogram after the completion of the first transaction is prohibited, in all cases, including for subscriptions requiring different payments. 4.1 Single payments and subscriptions The Commission specifies that: in the case of single payments (one-off purchases or subscription without tacit renewal, paid in one go), the retention period for data relating to the card must correspond to the period i necessary for the completion of the transaction, i.e. the actual payment which may be deferred upon receipt of the goods or the performance of the service, plus, where applicable, the withdrawal period provided for for remote sales of goods and supplies of services (Article L.121-20-12 of the Consumer Code); with regard to subscriptions involving installment payments, the retention of bank details is justified: until on the last payment due date, if the subscription does not provide for tacit renewal; until termination of the subscription in the event of renewal by tacit renewal, subject to the applicable provisions and in particular to the information of the persons concerned before renewal.4.2 Complaints managementWith regard to online merchants, the financial risk of unauthorized use ultimately weighs on them in the event that they have not implemented a system of authentication of their customers, the Commission considers that they can keep the card number and the date of validity of the latter when this retention is necessary for the management of any complaints from payment card holders. The data may be kept for the period provided for in Article L. 133-24 of the Monetary and Financial Code, in this case 13 months following the debit date. This period may be extended to 15 months in order to take into account the possibility of using deferred debit payment cards. transaction. Payment card numbers stored for this purpose must be subject to technical security measures, as described in Article 6 of this recommendation, aimed at preventing any unlawful reuse. 4.3 The fight against money laundering In cases where the data relating to the card would be collected by an organization subject to anti-money laundering obligations to offer a remote payment solution, they may be kept until the account is closed and then, if necessary, archived in accordance with the legal

obligations in this area.4.4 Other purposesIn cases where the card number is used for other purposes, as part of a simple option aimed at facilitating subsequent purchases, a subscription giving access to additional services or processing for the fight against fraud, its retention period may not exceed the period necessary for the fulfillment of this purpose. Article 5: The rights persons5.1 The general obligation to inform Any use of the payment card number, whatever the purpose, must be the subject of complete and clear information to persons. They must be informed of what will be done with their data, from the collection stage, under the conditions provided for in Articles 13 and 14 of the GDPR. They must be informed of how to exercise the rights: withdrawal of their consent or opposition to the processing of their data; access, rectification and erasure of data concerning them; limitation of processing; for example, when the person disputes the accuracy of their data, they can also request the temporary freezing of data processing while the organization carries out the necessary checks; portability: the data controller must allow any person to receive, in a structured format commonly used, all the data processed by automated means which would have been provided by the person on the basis of his consent or of a contract. It is therefore recommended to specify to the data subjects the processing concerned by this right. to oppose certain processing operations (such as the retention of data in the context of a subscription giving access to a privileged commercial relationship, for example) must also be provided for on the data collection medium. 5.2 Specific information when tacit renewal of the subscription With regard to subscription contracts with tacit renewal, the Commission recalls that the data controller is required to inform the data subject of the tacit renewal of his contract and, unless he objects, the conservation of his bank details for the payment of the installments of the new contract.5.3 Information and collection of consent during the retention of data for the purpose of facilitating subsequent payments When card data is retained beyond the time strictly necessary to carry out the transaction to facilitate subsequent payment, the Commission considers that this processing must have received free consent, specific, informed and unambiguous data subject, in accordance with the provisions of Article 6 of the GDPR. customer, in this case not having to re-enter his card number during a next purchase and/or allowing him to make a purchase in one click. Therefore, this data processing requires that the prior consent of the person concerned be obtained. This is not presumed and must take the form of an unambiguous act of will, for example by means of a checkbox (not pre-checked by default). The acceptance of the general conditions of use or sale is not considered as a sufficient method of obtaining the consent of individuals. In order to meet the obligation provided for in Article 7-3 of the GDPR, the Commission recommends that the responsible for processing integrates directly on its merchant site a simple means of withdrawing, free of charge, the consent

given. 5.4 Information and prior opposition to the storage of bank data in the event of subscription to a subscription giving access to additional services facilitating purchases, reflecting the customer's registration in a regular commercial relationshipThe Commission considers that the fact for a person to take out a subscription giving him access to additional services (fast delivery, access to private sales or additional content, etc.) may reflect the customer's intention to enter into a regular commercial relationship. In such cases, the Commission considers that the retention of bank data of the person to facilitate subsequent purchases may be based on the legitimate interest of the data controller, the person may, under these conditions, reasonably expect that their bank data will be kept to simplify subsequent purchases. However , in order to be able to validly rely on the legal basis of legitimate interest, the data controller must clearly inform the persons concerned, when entering their bank details on the dedicated medium, of their storage by default and of the duration of this storage. During this entry, the person must also be able to object, simply and at their discretion, by a visible, explicit and ergonomic means, such as a checkbox, to the storage of their bank details. The opposition expressed in this way must be taken into account by the data controller, including during subsequent purchases. may subsequently not retain by default the bank details newly entered by the customer during subsequent purchases. The recording of the bank details entered can only be carried out at the explicit request of the person concerned, expressed here again by visible, explicit and ergonomic means, such as a checkbox.Finally, the data controller must also allow individuals to request, at any time and at their discretion, the deletion of their bank data.Article 6: Protection measures securityThe Commission considers that the responsibility for the processing aimed at keeping the customer's card number in order to facilitate any subsequent purchases on a merchant site or for the payment of a subscription is in principle the responsibility of the merchant benefiting from the storage of data relating to the card, i.e. the one for whose benefit the transactions carried out with the stored data will be carried out. The service providers who store data relating to the card on behalf of the merchant have the status of subcontractor and are required to put in place appropriate security measures. The Commission notes that the practices relating to the collection of the card number payment card leads to the multiplication of databases that could potentially be the subject of fraudulent reuse, in particular in the event of a security breach leading to the compromise of this data. The Commission therefore considers that data controllers must strive to develop and adopt best practices and promote behavior that takes security requirements into account and respects the legitimate interests of individuals. In this regard, the Commission recalls that: Article 32 of the GDPR requires the controller to take security measures (technical and organizational) in order to avoid in particular any illegitimate access to data are

processed. These measures must be proportionate to the risks generated by the processing for the data subjects. Since unauthorized access to data relating to the card can lead to fraudulent transactions, the confidentiality of this data must be specifically protected; Article 28 of the GDPR requires the data controller wishing to outsource the management of the system to payment to choose a subcontractor with sufficient guarantees to ensure in particular the implementation of the security measures made necessary under Article 32 of the GDPR. The data controller and the chosen subcontractor are required to establish a contract specifying their respective obligations and containing the provisions of Article 28 of the GDPR. This being recalled, it recommends that: data controllers only use services secure online payment methods that comply with the state of the art and applicable regulations. In this respect, only devices that comply with recognized standards for securing data relating to the card at European or international level (for example, the PCI-DSS standard) must be used. The person responsible must also ensure that the processing complies with the requirements of the GDPR, in particular through the implementation of a risk management approach in order to determine the necessary organizational and technical security measures. To support data controllers in this process, guides Privacy risk management and Subcontractor's guide are available on the Commission's website; the data controller and its possible subcontractor(s) adopt a strict data management policy. authorizations of their personnel, only giving access to customers' payment card numbers when strictly necessary. Obfuscation measures (masking of all or part of the card number when it is displayed or stored) or replacement of the card number by a non-significant number (tokenization) must be implemented in order to limit the access to card numbers. The staff must be made aware of the risks of fraud in terms of data relating to the card and the security measures allowing them to be avoided; the data controller and its possible subcontractor(s) do not, under any circumstances, record data relating to the payment card locally, on the terminal equipment of their customers (such as computers or smartphones for example), and must not encourage the latter to carry out such registration, as this equipment is not designed to ensure the security of this type of data; the data controller and its possible subcontractor(s) take the necessary measures to protect themselves against any breach of the confidentiality of data relating to the card when these are collected via a service communication to the public online. Data passing through public communication channels or those liable to interception must in particular be subject to technical measures aimed at making this data incomprehensible to any unauthorized person; when data relating to the payment card are kept in order to facilitate the subsequent execution of transactions, the access or use of this data must be subject to specific traceability measures allowing any illegitimate access or use of the data to be detected a posteriori and to

be attributed to the person responsible; in addition to the notification of breach which must be addressed to the CNIL, the persons whose data has been the subject of a security breach are notified so that they can take the appropriate measures to limit the risks of fraudulent reuse of their data (dispute of payments fraudulent, opposition to the card, etc.); when the data relating to the card of payment are kept for the purpose of combating fraud, they must be subject to technical measures aimed at preventing any illegitimate reuse. These measures may in particular consist in storing the numbers of the payment card in hashed form with the use of a secret salt which is not kept in the same storage space; means of reinforced authentication of the holder of the payment card are put in place, aimed at ensuring that it is indeed the origin of the act of remote payment; when the collection of the payment card number is carried out by telephone, it is also necessary to implements security measures such as the traceability of access to card numbers. It recommends that a secure alternative solution, at no additional cost, be offered to customers who do not wish to transmit data relating to their cards by this means. will be published in the Official Journal of the French Republic. President I. FALQUE-PIERROTIN