The Dangers of a Loyalty Card

Investigating Offline Retailers' Loyalty Programmes and Data Protection

Leiden University
Faculty of Governance and Global Affairs
MSc in Crisis & Security Management

Master Thesis

Name: Daan Brok
Student number: s2413809
Supervisor: Dr. T. Tropina
Second reader: Dr. E. de Busser
Word count: 17.372 words
Date: 14 February 2020

Universiteit Leiden
Governance and Global Affairs

Abstract

This thesis presents an exploratory study of the data protection at offline retail organisations. Retailers gather a lot of (personal) data using loyalty programmes and are becoming sophisticated players in the field of data analysis. Customers willingly trade their personal data for personalised discounts or other perks when using a loyalty programme. This trade-off puts pressure on the retailer to provide adequate protection of their personal data, as it is reliant on its (loyal) customers to survive. When data is breached as a result of poor data protection measures, not only does the retailer risk large fines from privacy authorities, the retailer is likely to get a lot of negative PR, hurting its image. To examine what would constitute appropriate and sufficient data protection measures, GDPR article 32 (security of processing) and ISO standards 27001, 27002 and 27701 regarding information security were analysed. Then, the privacy statement and other publicly available information regarding privacy and data of three large Dutch chains were studied. Finally, interviews were conducted with major chains with loyalty programmes to gather more information on technical and organisational measures and their view on data protection and privacy. These were combined to form a matrix of sixteen requirements that constitute adequate data protection. While there was not enough information to test the matrix on one of the retail companies, it is clear that retailers are taking their responsibilities seriously, while at the same time eager to use the data to the fullest extent they are allowed to.

Key words: cybersecurity, data protection, GDPR, information security standards, retail, loyalty programmes

Table of Contents

1. Introduction

Approximately 7 million people in the Netherlands are in the possession of an Albert Heijn 'bonuskaart' (RTL Nieuws, 2018, par. 2), a card which gives discounts on different products each week. 4 million customers have used the Hema customer pass (Terra, 2018, par. 1), and 6 million people are gathering Airmiles in order to get discounts (Mast, 2018, par. 13). On a population of approximately 17 million people, this means retailers are gathering data on the purchases of a large chunk of the total population.

The customer card that we use in order to get discounts is the gateway for retailers to create a profile of us and our consumer habits. These are stored in databases which are used by retailers to personalise discounts, in order to get you to spend more money in their stores, to enable targeted advertising and to set up customer profiles in order to maximise turnover (Gomez et al., 2012).

Any data that is gathered and subsequently stored for future use is at risk of being stolen by cybercriminals. As the data that is collected by retailers through customer cards can form comprehensive profiles of individuals, this data is extremely valuable and at risk of data theft. Data theft means (personal) information is illegally copied or taken from a business and then (usually) resold (Saini et al., 2012). The data the stores you frequent have collected and linked to your personal profile is valuable and is thus at risk of being stolen and potentially abused.

Companies will try to frame using your data in a diplomatic, helpful way ("we only use your data to improve the services we provide"), however, the implications of your data being stole are extensive. What if health insurance companies get their hands on one of these databases, notices someone tends to not eat very healthily, and it decides to raise the premiums on that basis? This might be seen as an invasion of privacy and leave people questioning why and how much data they (sometimes unknowingly) share with the stores they frequent (Hill, 2012).

Scandals regarding data breaches can also have a large impact on a companies' business operations and reputation, and they will try to avoid privacy risks as much as possible (Hill, 2012; Rosen, 2019). On the other side, consumers want to be sure their data is safe with a certain organisation and trust that it will not be misused or stolen.

Academic and societal relevance

Extensive research has been done on data protection and data processing by online retailers (Chakraborty et al., 2016; Verhoef et al., 2015). It is relatively easy to gather customer data through online channels: customers have to create an account on the websites, or they can be tracked and a profile can be created from their credit card credentials, for instance. "Offline" retailers (chains with physical stores) that use loyalty programmes also gather and process a lot of (personal) data, however, there are few scientific articles on the safety of loyalty programmes' data. Cybersecurity and data protection by offline retailers have not been widely discussed in academic literature. All the while, offline retailers are said to be struggling to comply with all regulations (Rosen, 2019), making for an interesting, underexposed area of research.

Developments in the field of cybersecurity have taken a large flight in the last decade. Businesses have been using the latest technological developments in data gathering and analysis to inform high-level decisions. However, major regulation on the usage and protection of data has only been implemented relatively recently (Zerlang, 2017).

Adopted by the EU parliament in 2016, the General Data Protection Regulation (GDPR) came into full effect in 2018. The GDPR requires companies to ensure their systems are resilient and secure, to avoid data breaches wherever possible and to report on them when they have failed to prevent a data breach. According to Zerlang (2017), cyber-resilience will become much more important, as the understanding is growing that cyber-attacks will occur, no matter what. Under the GDPR, businesses themselves are responsible for proactively preparing for breaches and to soften the blows (and mitigate the leaks) caused by cyberattacks.

Research objectives

This research will look into to what extent (offline) retail companies have implemented data protection guidelines in their organisations and what they are doing to keep consumer's data safe.

Using article 32 of the GDPR and ISO information security standards as frames of reference, it will be investigated what retailers are required to do to ensure adequate data protection and negate the risks of processing the large amounts of personal gathered through loyalty programmes.

Using three case studies as well as interviews with three retailers, a 'matrix' will be set up, identifying requirements for adequate data protection to examine how retailers are protecting customers' personal data.

The case studies will be three retailers active in the Netherlands, focusing on the privacy and data protection of customers using loyalty programmes. These programmes are voluntary and consumers are willingly sharing their data in order to get discounts or other advantages. This makes them stand out from online stores, in which the store is gathering data on purchasing behaviour often without the customer realising.

Research question

This paper aims to answer the research question "To what extent have offline retailers with loyalty programmes taken action to comply with GDPR's data protection requirements and international information security standards?"

There will be sub-research questions to help answer the main question. These are as follows:

- "Which security requirements can be identified using article 32 of the GDPR and ISO security standards?"
- "What actions are retailers taking (or planning to take) to meet the recommended security requirements regarding data protection?"
- "What difficulties are companies experiencing in their efforts towards adequate personal data protection?"

Reading guide

This thesis will first conceptualise certain key terms in the area of cybersecurity, data protection and personal data. After setting out how the research will be carried out, the relevant sections of the GDPR and international information security standards will be examined. In the analysis, a set of requirements will be set up. These will be based on the GDPR and the security standards, as well as three case studies and information from interviews. The information from these different sources will be combined to form a matrix with requirements for adequate data protection.

2. Body of knowledge

Conceptualisation of key terms

This research mainly deals with the cybersecurity aspect of crisis and security management, more specifically concerning data protection. As discussed by Hansen & Nissenbaum (2009), up until the last decade, it had been a relatively underrepresented topic in security studies.

Cybersecurity is defined by Craigen and colleagues (2014) as "[the] organisation and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights". As they elaborate in their research, this shows the complex and interwoven dimensions of security in the cyberspace, while touching upon the fact that it is used for an incredibly wide variety of processes. (Craigen, et al., 2014). Lastly, it includes the fact that the notion of ownership and control is prevalent in the discussions regarding cybersecurity. In the words of Craigen, et al. (2014), this includes "access, extraction, contribution, removal, management, exclusion, and alienation". Thus, any theft or misuse of digital property (such as personal data), whether accidentally or maliciously, is a cybersecurity incident.

Data protection is a broad concept. Data has become a valuable commodity, and with that comes the need to protect it. Using (personal) data can present privacy concerns, and in order to create a balance between an individuals' privacy and the beneficial usage of data, several concepts must be addressed. The question what exactly entails personal data, the role of consent, data minimisation and purpose limitation must be looked at when addressing concerns about processing data (Tene & Polonetsky, 2011, p. 64).

General Data Protection Regulation. These concerns are (amongst other issues) addressed in the EU's General Data Protection Regulation (2016), and this paper will chiefly use article 32 of the GDPR as the starting point in what data protection entails. The GDPR was adopted by the European Union Parliament in 2016, and came into force in May 2018. It entails many aspects of privacy, including data breaches and privacy by design. Article 32 of the GDPR primarily deals with the security of data processing.

ISO standards. As organisations are using data and information systems more and more for their core business processes, effective data protection management becomes more important in order to prevent security breaches and reduce risks (Fomin, Vries & Barlette, 2008, p. 2). International standards have been developed to allow companies to ensure an adequate level of information security. ISO 27001, published in 2005 and adapted to new technical measures in 2013, by the International Organisation for Standardisation, is one of the international security standards dealing with information security.

The standard does not so much stipulate concrete measures, as it provides a framework with guidelines. The measures must be developed and implemented by companies themselves (Disterer, 2013, p. 95). In general, it promotes planning, implementation, operation and continuous monitoring and improving of any processes related to information security (Disterer, 2013, p. 95).

A related security standard is the ISO 27002, which provides control objectives and best practices for organisations on how to best implement security measures to ensure compliance with ISO 27001. ISO 27701 is another standard, published in 2019, which deals specifically with privacy in information management systems. It aligns with the obligations set out in the GDPR and other privacy laws around the world (NEN, 2019).

Compliance and risks. The usage of data in (commercial) decision making is becoming more common practice. Without proper security in place to protect that data, businesses can be faced with negative impacts, including "financial consequences, weakened protection of the organisation's intellectual capital, loss of market share, poor productivity and performance ratings, ineffective operations, inability to comply with laws and regulations, or loss of image and reputation" (Humphreys, 2006, p. 10). Even if the consumer experiences no direct (financial) harm, customers respond negatively to organisations collecting and using their (personal) data (Martin, Borah & Palmatier, 2017, p. 52).

In the literature, several barriers are given not to adopt or implement information security standards. Fomin, Vries and Barlette (2008, p. 10) state that reasons not to comply with ISO standards might include high resource costs in money and time for implementing the standards. Another reason might be a (perceived) increase in paperwork; however, they state that for ISO27001, this is not seen as a major barrier. An explanation for non-compliance with the GDPR was suggested to be the fact that privacy authorities waited with sanctioning for a while after the legislation was introduced (Scroxton, 2019, par. 6). This gave certain organisations the idea that the GDPR was "all bark and no bite" (Scroxton, 2019, par. 6). The

Dutch privacy authority stated it deliberately focused more on education and advising in the first year after the GDPR was implemented rather than enforcing and sanctioning (Autoriteit Persoonsgegevens, 2019, p. 19).

In case a company fails to comply with the GDPR, the data protection authority in the relevant country can start an investigation with the possibility of sanctioning the offender. The Dutch privacy authority in charge of GDPR enforcement, the Autoriteit Persoonsgegevens (AP) was notified of 20.881 data leaks in 2018, actively dealt with 298 of those data leak notifications and fined one company for 600.000 euros for failing to notify the authority in a timely manner (Autoriteit Persoonsgegevens, 2019, p. 18).

The Lithuanian Data Protection Authority investigated retail chains with loyalty programmes to see how they measured up to the obligations set out in the GDPR. Out of 12 cases investigated, 11 companies were found to be violating personal data processing regulations (GDPR Register, 2018, par. 3). Violations ranged from collecting an excessive amount of 'unnecessary' information to the terms of storage of personal data. The authority fined the companies on a probationary basis: it instructed them to eliminate the violations (GDPR Register, 2018, par. 9-10).

Personal data. The GDPR considers personal data to mean "information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Article 4(1) of GDPR, 2016).

The European Data Protection Supervisor (EDPS) summarises it as any information which relates directly to a person, while it might also include, for instance, e-mail addresses or a phone number (EDPS, 2016). In ISO standards, personal data is called PII, or personally identifiable information (ISO/IEC 27001, 2013). The definition in the ISO standards cover the same information as the definition used in the GDPR.

Loyalty programmes. Loyalty programmes are used by retailers to get customers to stick with their company, to make sure they return to their brand for their next purchase (Feiereisen, 2019, par. 3). The term loyalty programme can be seen as a variety of different marketing initiatives. It could be a physical card giving discounts, tiered service levels or special customer support methods. It is aimed towards "positively [influencing] consumers' attitudes and behaviours towards the brand or firm" (Henderson, Beck, & Palmatier, 2011, p. 3).

One of the main benefits of using loyalty programmes (to retailers) is their ability to provide useful data. This can include data on individual customers as well as general buying behaviour (Nunes & Drèze, 2006, p. 126). They can be used to attract new customers, but are used more often to retain existing ones and try to get them to increase their spending (Lakshmanan, 2019, par. 7).

To most retailers, the most (commercially) interesting aspect the data enables them to investigate is looking into the underlying behavioural processes that lead to purchasing items and predicting spending behaviours (Henderson, Beck, & Palmatier, 2011, p. 3; Nunes & Drèze, 2006, p. 125). Loyalty programmes can also provide insights into things such as brand loyalty or price sensitivity, as well as allow for segmentation of groups of customers (Rhoen, 2019, p. 7).

The information registered by your loyalty card when shopping might be supplemented with other databases; retailers can 'enrich' their databases by buying consumer data from data broker companies, in order to create a more complete profile of a customer (Lakshmanan, 2019, par. 14; Kreiken, 2016b, par. 5). In 2016, Bits of Freedom, a digital rights and privacy NGO in the Netherlands, found the legality of the conduct of data brokers to be questionable (using the principles of the then-newly introduced GDPR). There seems to be a chronic lack of transparency and data ownership is unclear (Kreiken, 2016a, p. 24). However, loyalty programmes or customer databases, even without additional data from data brokers, are considered to form a competitive advantage. They allow companies to identify consumer (groups) that are likely to return to their stores and become or stay loyal customers (Lakshmanan, 2019, par. 26).

Loyalty programmes do not necessarily make use of personal data. It depends on the programme and whether or not they ask customers to register. For instance, it might be possible to use a loyalty card as a way to get access to the discounts, without registering the card and linking it to your name or e-mail address. This would mean no personal data is recorded. For this research, only registered/activated loyalty cards will be taken into account. In the case

study analyses, it will be set out in more detail which information the different retailers ask for. However, invariably the customer's name and e-mail address are required to register, meeting the requirements to be considered personal data according to the GDPR.

Most loyalty programmes, even those that do not require registration, aim to link purchases made at varying moments to one customer. This allows retailers to analyse the purchasing behaviour at a larger scale than one transaction at a time, as it enables them to make a history of purchases over time. A list of purchases made by one entity, without any other identifying information, is not strictly speaking personal data according to the GDPR.

In a dissertation at Leiden University (Rhoen, 2019), it was argued that one of the major risks of big data include that which can be deduced from the data. In other words, while data gathered is not necessarily personal data, what can be inferred from it might be (sensitive) personal data. An example given is one of a person with a supermarket loyalty card who never buys pork and never does groceries on Saturdays. From that, it can be surmised that that person is likely Jewish (Rhoen, 2020, par. 16). This shows that while purchasing behaviour in and of itself might not be personal data, knowledge that is gained from scrutinising it might become personal data.

3. Research design

Conceptual model

The research will consist of four phases, as seen in figure 1. This figure is based on the research framework as set out by Verschuren, Doorewaard & Mellion (2010, p. 20). The first phase is an analysis of what article 32 of the GDPR and ISO information security standards prescribe and how companies can implement these standards. This desk research is translated into a preliminary table of requirements on how to safeguard customer data protection. Three case studies, along with interviews with retailers, will be used to 'test' this framework in practice and adapt and enhance it into a definitive matrix of data protection measures.

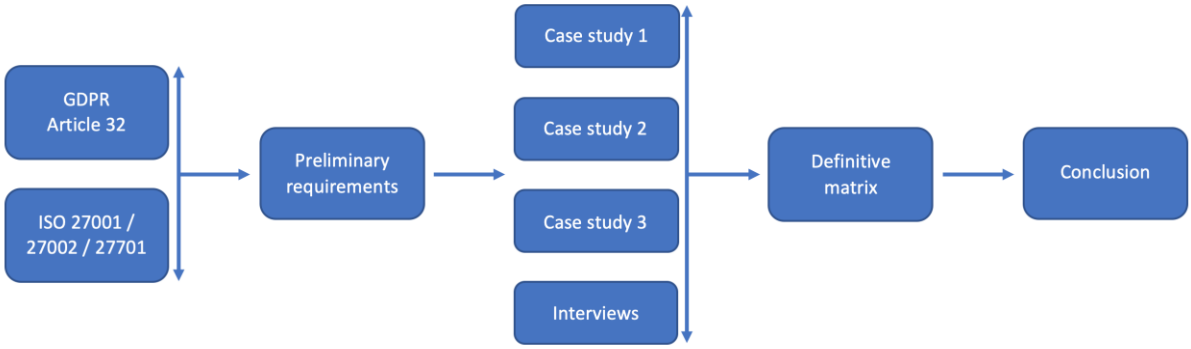

Figure 1 - Conceptual model.

Research design

According to Stebbins (2011), exploratory research should be done when there is little available work on a specific topic. It emphasises the development of theory from data, instead of "[emphasising] methodology and the actual collection of data by which this development is accomplished" (Stebbins, 2011). As the information regarding data protection and retailers' measures taken to keep malicious actors out of their systems is usually kept out of the limelight, this research will aim to create general findings that are open for future research, as well as providing companies with insights on the progress of the implementation of these security standards.

Case study

This research will consist of a multiple-case study. According to Bryman (2016), this is the comparative case study design usually used in qualitative research strategies. In short, it means that multiple similar cases are investigated. It enables an analysis of the same situation in different settings, multiple times. The case studies will be built up from data gathered from publicly available sources.

Interviews will be held with three retailers with loyalty programmes, not necessarily the same ones as the case studies. Data from the interviews will be used to inform the matrix.

Using descriptive research, case studies and the interviews will allow relatively detailed findings to be made regarding data protection measures.

Case selection

Primarily, the retail sector will be looked at. Data protection, privacy breaches and cybersecurity in general are topics that are highly relevant in many sectors. While it could be very interesting to see how, for instance, healthcare institutions, municipalities, insurance companies or financial institutions are dealing with these issues, for various reasons, the retail sector was chosen. First of all, the fact that organisations that are distinctly part of the *private* sector have a clear responsibility regarding cybersecurity and data protection makes for a more interesting research topic. Secondly, retail is not traditionally seen as a sector that handles a lot of personal data, while insurance companies or banks are.

In the last few years, retailers have started using data more and more, and with the heightened focus on data security and privacy, retail companies have many new responsibilities to safeguard. Data gathered by retailers, especially ones that are frequently visited (such as supermarkets or health and beauty stores/drugstores) can paint a clear picture of someone's consumer habits and in extension their daily life. Any data breaches in those databases would be an invasion of people's personal sphere.

This thesis will mostly look into *offline* retailers rather than *online* stores. Online stores can gather data relatively easily, for instance because people have to make an account and register before they can order something. For offline stores, it is more difficult to gather this data and create a customer profile: they usually have to use loyalty programmes or discount cards to get the same data, and even then, customers usually have to register themselves. People typically get the choice to use the customer cards, and they get benefits if they choose to do so. This means they "freely" give up their data. Coupled with the fact that there is little academic research done in this field, and how offline stores are not traditionally seen as actors that are active in the field of cybersecurity or data protection, this should make for a research topic that is interesting to explore. There is little literature to be found on data protection in combination with loyalty programmes and offline retailers.

The three specific case studies were chosen due to the availability of public information and/or because their loyalty programmes belong to the largest or most well-known in the Netherlands.

Data collection and measurement

Desk research will be done to investigate privacy and data protection guidelines, legislation and/or international security standards. Using that research, a framework will be created to assess the risks and measures to safeguard those risks.

Further, to gather data on practices, a set of questions will be formulated in order to structure interviews with stakeholders within retail organisations. In a semi-structured manner, three different organisations will be interviewed, all known to have a loyalty programme keeping track of customer's purchases.

During the interviews, the framework created using the international data protections standards will be used to assess to what extent the retailers have implemented these standards in their organisations and to enhance it.

Limitations

As for some of the limitations of this research, the following have been identified.

Construct or measurement validity has to do with whether a measure to look at a concept is actually measuring that concept (Bryman, 2016). It could be argued that compliance with article 32 of the GDPR and the ISO standards alone is not enough to make strong conclusions on the privacy or data breach risks, thus hurting the construct validity.

External validity deals with whether findings "can be generalised beyond the specific research concept" (Bryman, 2016). With only three case studies to base the results of this research on, the external validity might be low. A further issue in this area could be the fact that only Dutch retailers are taken into account, while the GDPR legislation is EU-wide and cybersecurity is a worldwide concern. However, the thesis will be able to discuss to what extent data protection measures have been implemented in the organisations, and it can be analysed to what extent the framework that was created was/is applicable there.

Reliability mainly deals with whether results of a study are repeatable, thus, if these concepts with repeated measurements remain consistent (Bryman, 2016). The reliability of this research, or specifically of the case studies is dependent on the answers received during the interviews; are they truthful, are they complete? This would need to be accounted for in the research.

4. Analysis: introduction

The analysis chapters are split up into several parts. First, article 32 of the GDPR and international security standards will be introduced. After that, combining the guidelines and regulations of these two, a preliminary matrix of requirements will be drafted. Using three case studies, as well as interviews, the matrix will be adapted and finalised in the final analysis chapter.

Introduction to GDPR

Under the GDPR, individuals must give their explicit consent for their data to be used, and one has the right to receive information on what data is processed by that organisation. Individuals can also require data to be removed if they believe is it no longer relevant or outdated, or for any other reason.

Companies must specify why they need data and what they will use it for. The scope of data protection under the GDPR is broad: any organisation in the world that deals with data of EU citizens needs to comply with the GDPR. In case of a data breach, organisations have an obligation to report it to the authorities within 72 hours. In case a company fails to do so, or fails to comply with any other part of the GDPR, sanctions can be very high: fines up to 4% of its global revenue for serious violations, or 20 million euros, whichever is higher. Every organisation that deals with data must appoint a data protection officer, and organisations that deal with a lot of personal data must make an impact assessment that details security measures taken to safeguard the risks associated with it (GDPR, 2016; Tikkinen-Piri, et al., 2018; Tankard, 2016).

GDPR Article 32.

This analysis will focus on article 32 of the GDPR; ‘Security of Processing’.

It requires organisations to “pseudonymise and encrypt personal data; ensure confidentiality, integrity, availability and resilience of processing systems and services; implement the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing” (GDPR, 2016, art. 32/1). It further requires assessment of all risks that are presented in processing; be it “accidental or unlawful destruction, loss, alternation, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed” (GDPR, 2016, art. 32/2).

Introduction to International Information Security Standards

Security standards exist to promote the best practices and requirements for (in this case) optimal data security. Standardisation allows companies, suppliers, regulators and others to assess security mechanisms to check whether they measure up to the standards set by an internationally recognised authority in the field, such as the International Organisation for Standardisation or ISO (ISO, 2019).

International standards ensure systems are implemented compliant with globally accepted security practices. Furthermore, information system standards give the advantage of a (global) consensus on terminology, enabling a common understanding and agreement of the requirements for systems, which strengthens interoperability between systems (ISO & CERN, 2014). This is advantageous when the data is processed by partners or using different suppliers. Adequate information protection might be required by business partners. Standards help to clarify quickly to what extent the organisation has proper data protection measures in place (Von Solms, 1999, p. 51).

Standards in the industry. There are various information security standards that all aim to provide benchmarks for adequate information security and to ensure the best security practices are adopted in an organisation. Five major information standards (identified by Susanto, Almanuwar & Tuan (2011)) are BS 7799, PCIDSS, ITIL, COBIT and ISO27001.

The BS 7799, which provided the basis for other standards, is published by the UK National Standards Body; ITIL is another security infrastructure standard developed on behalf of the British government. PCIDSS is an information security standard set up by the major payment card suppliers (such as Visa and MasterCard). COBIT is an IT governance framework that steers policy development and practices for IT regulation compliance. It is published by ISACA, an international professional association focusing on certification of information technology governance (Susanto, Almanuwar & Tuan, 2011, p. 27).

ISO/IEC standards. This analysis will chiefly use the ISO 27001, ISO 27002 and ISO 27701 standards. These are set up by ISO/IEC, two large bodies dealing with worldwide standardisation. They are non-governmental organisations, respectively called the International Organisation for Standardisation and the International Electrotechnical Commission.

The International Organisation for Standardisation has 163 national standardisation organisation members; these members can be part of a national government structure or be part of a private industry association. It was launched in 1947 and has issued over 22.000 industrial and commercial standards and norms (ISO, 2019, p. 5).

ISO and IEC provide security standards that companies can follow to be sure they are following the international best practices for (information) security. The security standards are set up by a joint technical committee of the two organisations, and then require approval of national bodies of members of the ISO and IEC (ISO/IEC 27001, 2013). The ISO 27000 series is concerned with information security standards.

For companies, regulatory pressure is increasing due to legislation such as the GDPR being implemented. Usage of data security standards can increase trust of customers in companies (Cooper & LaSalle, 2016, p. 23; Disterer, 2013, p. 92). Certification to internationally recognised security standards is an extra step to show that companies are taking active measures to prevent data breaches and to ensure maximum data protection, on top of regular, obligatory GDPR compliance. Certifications for one of the standards, ISO 27001, have increased more than 450% between 2008 and 2018 (IT Governance Europe, 2018).

In 2013, the ISO working group responsible for ISO27001 updated the ISO27001 standard and stated that the rise of new technologies and innovations required constant ‘vigilance’ regarding security measures, as users are using more and more websites and devices that handle personal data. This rise goes hand in hand with new security threats, increasing the need for constant updating and assessing whether the security measures in place are enough (Bird, 2013).

To further bring the measures in sync with the GDPR and other privacy regulations, ISO introduced ISO27701, an extension to ISO27001 that focuses on privacy information management; a management system for protecting personal data. The system as prescribed by the standard is focused on ongoing evolution and continuous improvement of data protection, “particularly important in a world where technology does not stand still” (Naden, 2019, par. 7)

ISO 27001. The standard ISO 27001 deals with the requirements for "establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS [Information System Management System] within an organisation" (Susanto, Almanuwar & Tuan, 2011, p. 24).

An ISMS is a system that aims to manage and protect an organisation's information, taking into account the confidentiality, integrity and availability principles. The ISMS is not just a database system, it encompasses the related procedures, policies, guidelines and controls that are used when pursuing the goal of a secure ISMS (Data Guidance, 2019, par. 4-5).

ISO 27001 is designed to allow organisations to select proportionate and adequate security controls for their ISMS. After its first iteration was published in 2005, the technical measures were updated in 2013. As of 2019, over 60.000 organisations have been certified to ISO 27001 (NQA, 2019).

The standard describes what requirements the ISMS must meet in order to be certified. It is an adaptive set of guidelines, aimed at companies in all different sectors and of whatever size. As ISO (2013) states, the implementation of the ISMS is influenced by "the organisation's needs and objectives, security requirements, the organisational processes used and the size and structure of the organisation".

ISO 27001 does not lay down concrete measures, as they must be developed specifically to meet the organisations' needs (Disterer, 2013, p. 95).

ISO 27002. While ISO 27001 sets out the requirements for certification, ISO 27002 provides guidelines for how to implement the required measures. It provides a tool to carry out the required risk analysis and provides measures to minimise the risks identified (Disterer, 2013, p. 95). ISO 27002 sets out the 'controls', provided in an Annex of ISO 27001, in extra detail. They are recommendations, summing up best practices in information management (Vreeling, 2018, par. 6).

ISO 27701. ISO 27701 is a new ISO standard that was published in August 2019. It was developed by the same technical committee as the two previously discussed standards, with input from external bodies such as the European Data Protection Board (IT Governance, 2019b, p. 4).

It is an extension to ISO 27001 and ISO 27002, providing requirements and guidance for privacy management and privacy information management systems (NEN, 2019). It deals with the privacy of personally identifiable information within an ISMS, and provides ways to

enhance an existing ISMS to address privacy requirements. It then becomes a so-called PIMS: a privacy information management system. It further sets out specific requirements for data controllers and data processors, a crucial distinction that is important in the European privacy legislation.

While it is not specifically based on the GDPR, it can be seen as a standard for compliance with the GDPR. One of the intentions of the new ISO standard was to align it with privacy legislation around the world including the GDPR (NQA, 2019; IT Governance, 2019b, p. 4).

5. Analysis: requirements

This chapter aims to set out which (personal) data protection measures can be identified using article 32 of the GDPR and ISO standards 27001, 27002 and 27701 as guidelines. It drafts a list of requirements for adequate data protection that retailers (and other organisations) would have to take into account. It aims to answer the sub-research question "Which security requirements can be identified using article 32 of the GDPR and ISO security standards?"

The organisational and technical criteria defined by the GDPR align quite closely with the mentioned ISO security standards. They will be discussed together in the following sections. Article 32 of the GDPR will be used as the basic structure for this chapter. This article of the GDPR is brief; it has four sub-articles and uses no more than 300 words. However, it outlines major information risk management principles very concisely.

General principles

Article 32 starts with the following paragraph: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk […]" (GDPR, 2016, Art. 32(1)).

First of all, it must be established who the controller and the processor are. In the definitions section of the GDPR, the following can be found: the controller is the person (or body, authority, organisation) who decides what the purposes and means of the processing of personal data are. The processor is the person (or organisation, et cetera) who actually processes this data on behalf of the controller. This is an important distinction. While the actual processing might be outsourced, the data controller is still responsible for what happens with the personal data, as the processor does so on behalf of the controller.

The first sub-article basically states that anyone who deals with personal data must look at any relevant processes or controls that are used in their industry or that are prescribed by standards and/or used by peers, while considering the effectiveness and costs of the implementation of these measures. Both the controller and the processor must protect the rights and freedoms of their employees, business partners as well as customers or other stakeholders. This must be done to safeguard risks, using both technical security controls as well as (organisational) policies and processes for employees, when 'appropriate'.

The appropriateness mentioned leaves room for adaptation of information management security controls that can be adapted to the size and needs of an organisation and the nature and context of its processing of personal data.

The following sections will set out requirements of adequate data protection, informed by ISO standards and the GDPR. Besides what it sets out in the GDPR, control objectives provided by the ISO 27001 and 27002 standards are used. These control objectives are specific guidelines, requirements or controls which the company can implement or adhere to in order to realise (certified) adequate (personal) data protection.

Requirement 1 – Pseudonymisation / encryption

GDPR Article 32 states that one of the measures organisations might take to ensure security of personal data processing is the pseudonymisation and encryption of personal data (GDPR, 2016, Art. 32(1a)). Pseudonymisation of data makes it more difficult to identify the individual behind the data. According to the UK Information Commissioner's Office, pseudonymisation and/or encryption of personal data is one of the primary recommended technical measures due its low implementation costs and widespread availability (ICO, 2019, p. 233). Pseudonymisation could be as simple as replacing a name with a unique identifier.

One of the controls set out in ISO27001 entails "[the protection of] the confidentiality, authenticity or integrity of information by cryptographic means" (Disterer, 2013, p. 96). Cryptographic means, in this case, refer to the encryption of data to secure it.

After a risk assessment, it can be identified which data should be encrypted. Not all data should be encrypted at all times, as the availability of data is a necessity which the standard values highly (NDC, 2018, par. 5). Each control in ISO 27001, such as encryption, must be based on the results of a risk assessment in order to pinpoint the assets (data) that are at risk and, in this case, should be encrypted (NQA, 2019, par. 49).

Requirement 2 – Maintaining confidentiality, integrity, availability, access

"The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services" is the second measure recommended in Article 32 (GDPR, 2016, Art. 32(1b)). Thus, all systems used for the processing of personal data or related services should be secure and resilient. This aligns with ISO 27001, which states that organisations should do thorough risk assessments to identify threats to its systems and to assure 'confidentiality, availability and integrity of data' (NDC, 2018, par. 6), and then take measures to reduce or eliminate those threats completely.

In short, all data should be available to users (processors) when needed, however provisions must be made to ensure that is not used or changed by unauthorised people, either maliciously or accidentally.

Confidentiality of data is crucial for customer trust; if data is leaked, or information in a database is (accidentally or maliciously) published, it might have grave consequences to the reputation of a company. The integrity and availability of personal data is essential as well, but more on the internal side of the data processing. If data is unreadable due to errors in the systems or files, or if the accuracy or completeness of the data cannot be guaranteed (anymore), this means the data has serious issues with its integrity. As for availability; if the data is safe, but the person who (legitimately) needs it cannot access it, it is considered not available. This creates unworkable situations for the processor: it cannot use the data for the purposes it is stored or gathered for.

Control objectives set out in ISO27001 include the objectives "[to] maintain the integrity and availability of information and information processing facilities", "[to] ensure the correct and secure operation of information processing facilities", "[to] control access to information" and "[to] prevent errors, loss, unauthorised modification or misuse of information in applications" (Disterer, 2013, p. 96). These directly concern the confidentiality, integrity, availability and access of data.

Requirement 3 – Resilience of processing systems and services / backups

The third measure mentioned to contribute to the security of processing is "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident" (GDPR, 2016, Art. 32(1c)).

In case a company is hacked, or is otherwise subject to a technical or physical security breach, there must be measures in place in order to safeguard and/or restore the availability and access to personal data, within a reasonable time after the incident occurred.

This is part of business continuity management (NQA, 2019, par. 52), something ISO 27001 provides controls for. These control objectives include "[the prevention of] errors, loss, unauthorised modification or misuse of information in applications" and the objective "[to] counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption" (Disterer, 2013, p. 96).

The measures in ISO 27001 aim to aid an organisation in keeping crucial data readily available in case of an interruption or breach in its systems. If this safeguard is managed well, a breach is likely to have little impact and the organisation is able to recover quickly.

In other words, companies must make provisions that in case of a damaging technical or physical incident, access to (personal) data can be restored quickly: necessitating (offsite) backups and other emergency strategies to deal with unforeseen events.

Requirement 4 – Regular evaluations and testing

The last of the four 'appropriate technical and organisational measures' as described in the first part of the Article 32 of the GDPR concerns evaluations and testing. In place must be "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing" (GDPR, 2016, Art. 32(1d)). In short, there must be processes that continually assess the effectiveness and performance of the implemented measures. Companies cannot 'blindly' trust their security policies and measures: they must proactively test them to ensure they work as intended.

According to ISO27001, organisations have to completely evaluate all possible vulnerabilities and risks that might potentially impact (personal) data. The security standard holds that the assessment process is crucial, and repeated risk assessments must produce similar results. If necessary, it should be adapted in order to ensure it remains up-to-date with current practices and usage within the company (NQA, 2019, par. 63). There have to be 'owners' of those risks and the risks should be evaluated and analysed regularly according to certain criteria. Compliance with these procedures should be monitored continuously (Disterer, 2013, p. 95)

Requirement 5 – Other technical/operational measures

The first four requirements mentioned are not the only measures available and/or necessary when it comes to data protection. Companies that use other measures, should evaluate it according to the following criteria: state of the art, processing profile, risk profile and cost, according to the first paragraph of GDPR Article 32 (GDPR, 2016, Article 32(1)).

This means only the most recent technology suffices and the newest tools and methods must be used when securing personal data, and this must be monitored and evaluated regularly in order to be compliant.

The risk profile should evaluate what the risks to the rights of a data subject are when their personal data is processed. The cost should assess what the implementation of the security

measures would cost, relative to the risk profile (GDPR, 2016, Article 32(1); Imperva, 2019, par. 5-8).

In GDPR Recital 78, an indication of what other technical or organisational measures could be appropriate is given. This includes concepts introduced in other articles of the GDPR, such as the minimisation of personal data, transparency regarding the usage and processing of personal data, the ability to monitor data processing by the data subject and the pseudonymisation of personal data as soon as possible (GDPR, 2016, Recital 78). In general, the data controller is encouraged to adopt "internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default" (GDPR, 2016, Recital 78).

Requirement 6 – Data breach protection

After listing appropriate measures to ensure security of processing, GDPR Article 32 goes on to state that "in assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed" (GDPR, 2016, Article 32(2)).

Thus, data being accessed, used, stolen or corrupted by any actors other than the intended processors would constitute a data breach. ISO27001 and ISO27701 are designed to prevent data breaches and protect against attacks targeting (personal) data. Quick identification of data breaches is one of the key necessities to ensure proper data protection, according to the ISO standards. One of the ISO27001 (and by extension, 27701) controls entails the efficient management of security incidents, enabling companies to respond faster to any data breaches and notify authorities of the breach (Bouca, 2016, par. 10).

Two specific ISO27001 control objectives dealing with data breaches are "[to] ensure authorised user access and to prevent unauthorised access to information systems" and "[to] prevent unauthorised user access, compromise or theft of information and information processing facilities" (Disterer, 2013, p. 96).

The GDPR, in articles 33 and 34, respectively, identifies the obligation to notify a supervisory authority and the data subjects of any personal data breaches. The mandatory notification is, potentially, a costly business for organisations: besides the costs for customer service operations, fines to regulatory supervisors and other legal fees, data breaches are likely to be harmful to a company's reputation (Karyda & Mitrou, 2016, p. 7).

The first four requirements will likely be major steps on the way to protection against data breaches. Article 32 of the GDPR stresses the importance of assessing the risks to personal data when the data is breached, to emphasise the data processors' responsibility in ensuring an appropriate level of security. Thus, this requirement builds on the other requirements.

Requirement 7 – Certification

The third article of GDPR Article 32 states that adhering to an approved code of conduct or certification mechanism can be used to demonstrate a company's compliance with the requirements mentioned in the Article (and discussed here in Requirements 1 through 5) (GDPR, 2016, Article 32(3)). It refers to GDPR articles 40 and 42 to further set out what Codes of Conducts or Certification bodies should entail to be in line with this Article of the GDPR. For instance, a Code of Conduct needs to be approved by the designated national privacy authority, and a Certification can only be provided by bodies that meet a number of strict criteria.

In the Netherlands, a Code of Conduct was officially approved by the Dutch privacy authority (AP) in August 2019 regarding obligations for data processors (AP, 2019, par. 1)

While no certification bodies are identified in the articles of the GDPR, the European Data Protection Board uses the definitions provided by the International Standards Organisation, or ISO, to inform their guidelines on how to be in line with GDPR in this aspect (Kamenjasevic, 2018), indicating ISO certification is one of the ways in which to be certified in being compliant with the GDPR.

ISO 27701 was specifically designed to enable companies to be certified compliant to the GDPR. In order to become and stay certified to ISO 27701, as well as 27001, organisations regularly receive audits from an accredited certification body, in order to be sure their information management systems meet the standards. This helps to ensure the systems are up-to-date with the most recent technology, but regular (internal) evaluations and tests should be carried out as well (NQA, 2019, par. 53-54; Naden, 2019, par. 4).

Requirement 8 – Controller instructions

The fourth and last part of Article 32 of the GDPR state that both the controller and the processor will ensure that no employee of either party, with access to personal data, processes that data unless on specific instructions from the controller. An exception is made for when the person is required to do so by law (GDPR, 2016, Article 32(4)).

Controls in ISO27701 and ISO27001 provide for this. Under ISO27001, businesses are obligated to control access to information and to ensure unauthorised access is impossible to any part of the database (Disterer, 2013, p. 96). Companies must limit access to (personal) data and data processing facilities, and provide for adequate authorised user access management to prevent unapproved access to systems. This also means that any third parties that are granted access to the personal data of one company, must make sure to adhere to the strict instructions of the data controller.

Requirement 9 – Security awareness

A crucial component of the successful implementation of data protection measures is the security awareness of employees. Within an organisation, it is vital that staff knows how to handle (personal) data in accordance with the law and security standards and knows the importance of data protection.

The GDPR does not comprehensively deal with this, however, "increasing employee awareness for data protection and training them accordingly" is one of the tasks prescribed to data protection officers (GDPR, 2016, Article 39(1b)). Creating awareness of the importance of data protection can prevent 'insider errors': malignant employees or employees making mistakes can be considered the hardest part of security (Irwin, 2019, par. 12).

ISO27001 provides controls that aim to manage this 'people problem'. These include training staff and policies or technologies that limit access to different levels of sensitive or personal information. In order to increase legitimacy for the procedures and policies, generating awareness is necessary. This must include any person who might process personal data. Disterer (2013, p. 95) states: "Adequate training should be developed for the implementation [of data protection measures] in order to push though the stipulated procedures and to establish them, and to generate awareness of their necessity". This comes back, for instance, in the following ISO27001 control objective: "[to] ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error" (Disterer, 2013, p. 96).

Requirements summarised

These requirements together result in the table below. This is considered the preliminary matrix of required data protection measures.

	Requirement	*Short explanation*
1	Pseudonymisation & encryption	Personal data should be encrypted/pseudonymised
2	Maintaining confidentiality, integrity, availability, access	Data should be available to processors when needed, but it must be protected against changes by unauthorised people, either maliciously or accidentally
3	Resilience of processing systems and services / backups	Provisions must be made that in case of technical or physical incidents, access to (personal) data can be restored quickly, necessitating emergency measures such as backups
4	Regular evaluations and testing	Security measures and policies, as well as all possible vulnerabilities and risks to (personal) data should be tested proactively and evaluated regularly
5	Other technical/operational measures	Other technical or operational measures are necessary for adequate security: these should use state-of-the-art technology, and the scope and purpose of the data processing must be assessed using risk profiles
6	Data breach protection	All technical or operational measures must be implemented to prevent data breaches, and adequate measures must be in place to respond to incidents should they occur
7	Certification	Adhering to a code of conduct or an internationally recognised certification body is recommended to demonstrate compliance with all security regulations and keep data as safe as possible
8	Controller instructions	Data can only be processed on the strict instructions of the controller, and the controller must make sure any third parties are taking steps to ensure they adhere to the standards set by the controller
9	Security awareness	(Information) security awareness is crucial to ensure adequate data protection, compliance and to reduce risks of human error/other security incidents in organisations

Table 1. Summarised requirements/preliminary matrix.

6. Analysis: case studies

In this chapter, three major retail chains and their loyalty programmes will be looked into. They are all based in the Netherlands. Two of the case studies are grocery stores/supermarkets and one is a department store. The three chains all currently have loyalty programmes and they work in a similar way: in short, customers have a card or an app, they scan their card at the check-out and in return they either get discounts or points to spend on discounts or free products.

The three chains have all been active for a long time (for 133, 93 and 40 years, respectively), however, they have introduced their loyalty programmes at different times in their history. Albert Heijn has been using its card for over 20 years, Hema for a little over 3 years and Jumbo is only just taking the first steps. This impacts what can be found about certain retailers and how much has changed or has been published in terms of publically available information.

Case study 1: Albert Heijn Bonuskaart

This section will analyse the loyalty programme of a major supermarket chain in the Netherlands; Albert Heijn. It currently has the most stores of any grocery chain in the Netherlands, in terms of quantity as well as square footage (Retailnews, 2020).

Introduction and history

Albert Heijn introduced its so-called Bonuskaart programme in 1998, becoming one of the first retail companies to gather data on its customer's purchasing behaviour digitally on a large scale (Heilbron & Koopman, 2019, par. 2). The Bonuskaart allows customers to purchase grocery items with a discount which they would not get if they do not have the loyalty card. Albert Heijn asked for data such as the name, address, date of birth and family composition. However, not long after its introduction, the Dutch privacy authority stated the grocery chain did not follow privacy regulations as they did not make clear why they were gathering the personal data and that customers were not obligated to provide the information (Heilborn & Koopman, 2019, par. 3). As a compromise worked out with the privacy authority, Albert Heijn introduced the anonymous loyalty card as an alternative. It functions the same way as the regular Bonuskaart, but customers do not have to give out their personal information.

In 2013, Albert Heijn introduced their new Bonuskaart. The old database had been 'corrupted': customers were sharing their Bonuskaart with others and employees were using their own cards when a customer had forgotten their own. This meant the data did not

accurately portray the purchasing behaviour of individual customers and could not be used for personalisation (Deibel et al., 2015). To start with a clean slate (and to start building a usable database), Albert Heijn introduced their new Bonuskaart, offering personalised discounts for the first time since the start of the programme. It also allowed one master Bonuskaart to be scanned at the register when a customer does not have or has forgotten their card: the data from those transactions does not enter into the main database (Deibel et al., 2015).

The retailer asked all of its customers to trade in their old Bonuskaart for the new one. This new card enabled customers to register their cards online, rather than just in the store. It aims to give discounts on products that the customer buys regularly or products which Albert Heijn thinks would fit their lifestyle based on a comparison with customers that have similar purchasing behaviours (Emerce, 2013, par. 2-3)

It is unclear exactly how many Albert Heijn loyalty cards are in use, and how many of those are personalised. In 2014, it was estimated that approximately 25% of customers had personalised their Bonuskaart (Retailnews, 2014a, par. 3). In another interview, Albert Heijn stated that approximately 2,8 million cards had been registered in the first year after the introduction (Retailnews, 2014b, par. 2). In 2018, it was reported that 7 million people regularly used the Bonuskaart, either anonymously or personalised (RTL Nieuws, 2018).

How it works

Albert Heijn loyalty cards are freely available at every Albert Heijn supermarket. Users can then choose to register that card online or using the Albert Heijn app, or continue to use it anonymously by not registering it. Users can also download the Albert Heijn app and use that as their Bonuskaart, but if they choose to do so they cannot use the programme anonymously, as it requires an Albert Heijn account (Albert Heijn Bonuskaart, n.d.)

By scanning the Bonuskaart at the register, the purchases are linked to the Bonuskaart number. If a customer forgets to bring their Bonuskaart, the employee at the register can scan a generic Bonuskaart or enter a code that allows the customer to receive the ‘Bonus’ discounts. However, this means the products are not linked to the user’s account and no personal discounts are granted.

On their website, Albert Heijn states that the more often a customer scans the loyalty card, the more they get to know you and the better able they are to give relevant discounts and other extras (Albert Heijn Bonuskaart, n.d.). On the Bonuskaart website, the following uses are unique to a personal loyalty card: getting personalised discounts, trying out new products for

free when they fit your purchasing history, and offering recipes based on your personalised discounts, amongst other (smaller) things.

When switching from an anonymous (unregistered) loyalty card to a personalised one, Albert Heijn uses your purchasing data from the past three months before activation to inform the personalised discounts it will offer you (Albert Heijn Bonuskaart, n.d.)

Personal data

When creating a profile in order to activate/register your Bonuskaart, Albert Heijn asks for your personal data. It asks your gender (sir/madam), first and last name, postal code, house number (using the last two to match with a public database to find your street name), your email address, your telephone number and your date of birth. It is mandatory to provide this information in order to activate your account.

To complete your account, it also asks you to choose a password. If you already have a Bonuskaart, you can fill in your Bonuskaart number while creating the profile. (Albert Heijn Bonuskaart, n.d.), otherwise Albert Heijn will give you a new Bonuskaart number. It is also possible to add other loyalty cards to your Bonuskaart account. Liquor store Gall & Gall (sharing a parent company with Albert Heijn) and loyalty programme Airmiles are partnered with the Bonuskaart programme. While Albert Heijn offers products of health & beauty shop Etos on their website, and they are both owned by parent company Ahold, they do not share data of their loyalty programmes (Etos, 2019).

In the media & controversies

According to an interview with Albert Heijn's director of omni-channel marketing and format, the retailer believes it can predict about 80 to 90 percent of the content of a customer's shopping cart before it enters the store (Retailnews, 2014b, par. 1).

In 2013, after the introduction of the new Bonuskaart, there was controversy surrounding the accessibility of purchase histories of loyalty cards. If a number of a Bonuskaart was known, regardless of it being anonymous or personalised, the entire purchase history of that card could be consulted via URL manipulation. A large Dutch consumer organisation argued that the purchase history of customers should be considered to be personal data and should be secured in the same way as other personal data (Consumentenbond, 2013, par. 1). However, Albert Heijn said that according to the current (in 2013) privacy laws, purchasing data is not considered to be personal data, so there was no legal issue there (Consumentenbond, 2013, par. 3). Privacy watchdogs disagreed, and stated that every consumer has the right to

keep his or her purchasing history anonymous and shielded from others, as this history might reveal personal details the customer does not wish to share. (Privacy First, 2013, par. 2-3)

In 2018, controversy arose when it came out that Albert Heijn used customer profiles in its new employee training programme which included what some thought to be racial stereotypes (Staalduine, 2018, par. 2). According to the retailer, these customer profiles were made to adapt the store's product range to the wishes of the customer and make clear to employees what customer profiles were made to make these decisions (Staalduine, 2018, par. 9). These profiles were likely set up using customer data from the Bonuskaart programme, as it allows Albert Heijn to create profiles of those who visit their stores and adapt their store presentation and product range to meet their needs.

Privacy notice

This next section will look at the privacy conditions of the Albert Heijn Bonuskaart. Albert Heijn has made their privacy statement quite accessible: it has a separate webpage (ah.nl/privacy) where it lays out the different ways in which the company gathers and processes data. The website uses clear language and has a logical build-up and navigation. The content is the same as the .pdf file of the privacy statement, which can be found on the same webpage.

The privacy statement is quite extensive: it consists of 61 pages of text as it includes all services Albert Heijn provides. For each service, it is set out which data is used, what the goal of the processing of that data is and for how long the data is saved.

This next section will provide an overview of the relevant parts of the privacy statement (Albert Heijn Privacybeleid, 2020).

Usage of data. Section 4.2.7 deals with analysis and advertisements. When shopping in Albert Heijn stores using a Bonuskaart, it states the information of your purchases is linked to your loyalty card. In case the Bonuskaart is registered and personalised, Albert Heijn will link that information about the purchases to the information it already has about your previous purchases, preferences and usage of online Albert Heijn services. The privacy statement states it uses this information for analyses and segmentation, while also using the information for personalisation of the website and communications towards the customers, as well as personalised advertisements and discounts.

Albert Heijn references segmentation, which can also be understood as profiling. Based on the data it has gathered on a customer, it will place them in one or more segments; groups that have certain common traits (Albert Heijn Privacybeleid, 2020, art. 4.3.1). These segments are used to personalise discounts, advertisements and communications or campaigns.

In section 4.4.1.3, this segmentation is elaborated upon. It uses a third company, Whooz, to analyse customers' needs. This company uses information from public databases such as the Dutch Centraal Bureau voor de Statistiek (Statistics Netherlands), the public Land Registry as well as the Chamber of Commerce to predict traits, interests and behaviours of all Dutch households.

The logic behind the choices of personalisation differ (Albert Heijn Privacybeleid, 2020, art. 4.3.1/art. 4.3.7.2). It might be products that are similar to things other customers in the same segment buy, products the customer has not bought in some time or products that are similar to things already bought.

Section 4.4.1.3. is perhaps most interesting when it comes to what Albert Heijn specifically does with your personal data. It states it analyses market trends using statistical analyses in order to 'evaluate' their product range, locations and marketing. These analyses, the section states, are only done by authorised employees who do not have access to the purchasing history and not the link to the Bonuskaart numbers or other personal data. The results of these analyses are only reported in an aggregated way, and cannot be traced back to individuals.

This section also states that it uses 'customer insights' gathered by third parties, including a company that uses, amongst others, a popular weather app to gather the location of its users. Using this data on locations, Albert Heijn aims to do research into customers' behaviours in shopping areas and the effectiveness of their marketing.

Purchasing data linked to a Bonuskaart is saved for 27 months, after which the link to a Bonuskaart number and other personal data is encrypted and the data can be used for another 4 years in order to analyse trends, but not linked to a customer's individual account.

Third parties with access to data. The privacy statement then mentions the third parties that might access personal data that Albert Heijn has access to (Albert Heijn Privacybeleid, 2020, art. 5). For all services that third parties provide such as IT maintenance, advertisements, website analytics and other things, Albert Heijn functions as the controller of the data. Albert Heijn is responsible for ensuring proper technical and operational measures to ensure adequate data protection and to ensure the data is only processed for the goals set out in the privacy policy. It lists four other companies that are engaged in order to analyse your data and personalise the website, communications, advertisements and discounts.

Protection of data. In the sixth main section of the privacy statement, Albert Heijn states they have taken the necessary technical and operational measures to protect personal data against loss or unauthorised use. Of note is that they mention the specific standards they adhere

to when it comes to information security: the ISF Standard of Good Practice for Information Security and COBIT (Control Objectives for Information and related Technology).

The ISF (Information Security Forum) Standard is a tool that provides all-round security coverage and assessments, and includes the controls set out in ISO27001 and ISO27002 (ISF, 2018). COBIT (2019) is a framework that deals with how organisations manage their IT systems. It is similar to ISO 27001, however, COBIT deals with IT overall, while ISO27001 chiefly relates to (information) security (Allport, 2019).

Conclusion

Albert Heijn has an extensive loyalty card programme, which is well-used. It is ahead when it comes to personalisation and profiling. It is very open about what it does with customers' personal data, allowing a lot of insight into what data they gather and combine in order to analyse their customers' purchasing behaviour. They privacy statement is extensive and the privacy section of their website is very user-friendly.

Case study 2: Meer Hema

This section will analyse the loyalty programme of a major department store chain in the Netherlands: Hema. It has over 500 stores in the Netherlands (Retailnews, 2020).

Introduction and history

In January 2017, Hema launched its loyalty programme called 'Meer Hema'. The programme entails both a physical as well as a digital customer card. Hema had for some time resisted introducing a loyalty programme, as it felt it did not fit the store's image (Vermeulen, 2018, p. 177). In 2016, Hema introduced a new strategy for their future, which was focussed on 'revitalising' their home market. According to their Chief Marketing Officer at the time, a loyalty card fit with that theme: a loyalty programme allowed Hema to get to know their customers better and use those insights to communicate better and adapt the experience and product range of their stores (Distrifood, 2017, par. 5).

The programme was successful in terms of users quickly: in the first month after its launch, a million customers signed up and four months after its introduction, almost two million people had used the customer card. A year into the programme, three million users were registered and in 2019, 4.5 million customers had used the Meer Hema card. (Toonen, 2017, par. 2; Terra, 2018, par. 1; Wierenga, 2019, par. 3). Of note is that approximately 1,1 million customers actively use their cards (HeyHema, 2019, par. 4). Hema found that users wanted to

use the card as they felt connected to the brand and wanted to feel ‘part of it’ (Oosterhout, 2017, par. 11).

Six months after the introduction of the Meer Hema programme, Hema’s (new) CEO admitted the retailer was relatively late with the introduction of a loyalty programme. They had the data for their online customers, but not the customers shopping in the physical stores, which still made up the vast majority of their turnover. However, according to him, the late introduction allowed Hema to avoid the pitfalls of previous loyalty programme introductions (Goslinga, 2017, par. 12)

With the data provided by the loyalty programme, Hema aims to better market to specific customer groups. They distinguish eight different customer groups with unique profiles, and use the loyalty programme to make sure they send more relevant communication. In the future, it will also offer personalised discounts (Goslinga, 2017, par. 2). Before the introduction of the loyalty programme, the store could only use the data of digital customers. Using the new data, the store aims to specify the customer groups and segments more and find ‘customer missions’: to better understand why someone visits the store (Voorn, 2017, par. 3)

As Hema offers a wide variety of goods and services, both online and offline, the loyalty data makes it easier to present cross-selling opportunities. Examples given include a customer buying new bed linen in the store, who could be given the suggestion to buy a Hema mattress online; or someone buying insurance for their bike who could be nudged towards buying a new bicycle bell or bike lights (Goslinga, 2017, par. 3; Oosterhout, 2017, par. 14). Currently, offering personalised discounts/vouchers for specific groups of customers are in the works, but are not yet implemented at a large scale (HeyHema, 2019, par 12).

How it works

The Meer Hema card can be scanned using a physical card or a QR code that is scanned using the Hema app. According to Hema, approximately a quarter of users under 40 use the physical card, contrasting with three quarters of users over 40 preferring the physical card (Toonen, 2017, par. 11).

During every transaction made in which the customer scans their Meer Hema card, one point is collected for every euro spent. These points can be used to buy vouchers that give discounts on certain Hema products. There are also certain discounts that are only valid with a Meer Hema customer card. Customers do not need to spend points for these (Hema, 2017, p. 13).

At the start of the programme, Hema gave out a mix of 10 different vouchers every month and was planning on personalising vouchers more as the programme developed and more customer data was available (Toonen, 2017, par. 13). However, as of 2019, the vouchers do not change monthly anymore. Instead, there are three basic vouchers for discounts or a free cup of coffee available at all times, with extra vouchers being introduced during special promotions (Hema, n.d.).

During those special promotions, generally twice a year, certain free products can be bought with the Meer Hema points, or they can be 'donated' to a charity picked by Hema. If a customer chooses to donate their points to a certain cause, Hema will do something for that cause for every voucher 'bought'. For instance, in 2019-2020, Hema donated a children's book to food banks for every voucher bought with that purpose (Hema, n.d.).

During the week of the customer's birthday, customers can pick up a free tompouce (a Dutch pastry). According to the head of the loyalty programme, vouchers such as a free cup of coffee provide up to 25% higher spending in the restaurants, and the free tompouce usually goes home with 2.5 more paid tompouces and approximately 18 euros of other Hema products (Wierenga, 2019, par. 6)

Every year, in the last week of January, the points the customer saved in the previous calendar year expire (Hema, 2017, p. 13). The head of the loyalty programme explained that Hema does this for financial reasons; most programmes that use points have these expiry moments, but they do not always acknowledge that publically or let the customer know proactively when they expire. Hema chose to do this in a transparent way, once per year (HeyHema, 2019, par. 7)

Personal data

The customer card can be used anonymously if a physical card is bought (for 50 cents) in the store and used only for purchases in the physical Hema stores. In that case, the customer can make use of the special discounts for Meer Hema customers, but cannot use the points to buy vouchers for more discounts or free products. In order to do so, the card must be activated by registering it, linking it to an account. This is also the only way to use the card digitally, using the app (Hema, 2017, p. 13-14).

When creating a profile in order to activate the Meer Hema card, Hema asks for personal data. It asks for gender (sir/madam), first and last name, date of birth, country of residence and the postal code and house number in order to find the street name. This information, along with an email address and a password, is mandatory in order to complete

the registration (Hema, n.d.). Optionally, a phone number and a company name can be provided. In case a customer already owns a physical card, they can enter their card number in order to link it to the account.

Privacy notice

The Privacy statement by Hema is relatively compact and short, but it is written in an accessible way. In the introduction to the statement, Hema states that it aims to be 'transparent, personal and trustworthy' (Hema, 2019, par. 2) when it comes to privacy and the processing of personal data. The statement can only be viewed in-browser and it does not clearly state the date when it was last updated.

Usage of data. The privacy statement indicates Hema uses personal data when making a Hema customer account. It distinguishes between an account linked to Meer Hema and one that is not linked to the loyalty programme. The only difference is that for a Meer Hema account, the customer is obligated to give their date of birth. The other data (address, name et cetera) is necessary for both types of account (Hema, 2019, section 1.1).

For the Meer Hema loyalty programme, the privacy notice distinguishes two levels of registration (Hema 2019, section 1.3). Level 1 is a customer who only has a physical pass, does not register it online and only uses it for the generic Meer Hema discounts. They do collect points but they cannot redeem them. This is the anonymous version of the programme.

Level 2 means the customer has to register their card; after that they will get full access to the programme. By registering, Hema gets full and unequivocal permission to analyse the customer's purchasing history and behaviour on Hema(-affiliated) websites.

In the fourth section of the part on data usage, Hema states it will use customers' personal data for statistical analyses in order to 'deliver websites, apps and services of the highest quality' (Hema, 2019, section 1.4). In order to conduct these analyses, Hema collates the customer's behaviour on their websites and regarding marketing outlets (newsletters or advertisements), as well as other data related to the customer's purchasing history. This includes any past products bought, webpages visited and other data gathered from the account or cookies. With the customer's permission, Hema can also use data from other parties (Hema, 2019, section 1.4).

In order to provide personalised discounts or advertisements, the privacy statement indicates Hema uses profiling, in their words "any form of automated data processing in which

certain personal aspects of [the customer] are analysed to predict, amongst other things, your personal preferences, interests and behaviour" (Hema, 2019, section 1.4).

Third parties with access to data. Hema uses third-party providers for services such as payment processors, marketing activities, website analytic, IT services and customer service. Hema always serves as a controller if the third party needs access to the personal data in order to provide their services (Hema, 2019, section 3).

Protection of data. Hema's privacy statement relatively short. It uses the generic sentence that it takes "appropriate technical and operational measures in order to protect personal data against loss or unauthorised processing" (Hema, 2019, section 4). The retailer does, however, add that it uses a protected SSL-connection during the ordering process and with contact forms.

Conclusion

Hema's loyalty programme has not been around for as long as the Bonuskaart programme has, but has gathered a lot of users in a relatively short amount of time. It asks for the same amount of personal data as Albert Heijn. It currently offers personalisation in communication, and is still developing personalisation on a larger scale, to be implemented at a later date. Contrasting with Albert Heijn, Hema's privacy statement is very brief and to the point. They are not open about whether or not they use other data to supplement their own database, it is not mentioned in the privacy statement. Hema offers next to no supplemental information besides the minimum, although it is written in an accessible manner.

Case study 3: Jumbo Extra's

This section will analyse the loyalty programme of a supermarket chain in the Netherlands; Jumbo. Still a family business, it is the second largest supermarket chain in the Netherlands in terms of market share, as well as number of stores, with over 650 stores currently operating (Retailnews, 2020).

Introduction and history

Compared to the other two retailers, Jumbo is only just starting out with its loyalty programme. While it has been active for over 35 years as a supermarket chain, it had never had a loyalty programme. One of the beliefs of the founder of the Jumbo chain was that "you'll

have the most successes if you do what the customer wants" (Vlems, 2014, par. 9) and this included having *everyday low prices* rather than having discounts and customer cards.

However, as the family business was taken over by the new generation, and the retailer bought other supermarket chains and incorporated them into their own brand, this view seemed to change (Vlems, 2014, par. 7). Now, a loyalty programme was no longer taboo, as it was felt the programme could be used in a way that benefitted the customer (by offering personalised discounts), without being too much nuisance.

In the second half of 2018, Jumbo started testing a new loyalty programme called Hallo Jumbo. In nine supermarkets, it started a pilot in which customers could scan a code in an app or a physical card and save points, which could be traded in for a set discount. According to Jumbo, it was an app that aimed to gather insights on the opinions of customers on saving for discounts on products (Jansen, 2018, par. 5). It was used to collect feedback on how to best serve the customer's needs.

Jumbo's CFO indicated it did not want the loyalty programme to be too similar to its major competitor Albert Heijn (Schrameyer, 2019, par. 3). The CFO also indicated it realised that Jumbo was not (yet) a major player when it came to collecting customer data, but it believed it was not inferior to its competition when it came to analysing data from the registers, albeit on an anonymous basis (Schrameyer, 2019, par. 4). The new loyalty programme would allow Jumbo to monitor individual customers' behaviour.

In April 2019, the pilot ended, with the announcement that the test was "a huge success" and the store would start working on a final version that would be used for all customers rather than just the 9 stores it began with. Jumbo did not give an indication when they wanted the full programme to go live (Garstenveld, 2019, par. 4-5).

In December 2019, the new version of the loyalty programme was ready and began its initial rollout. It was now called Jumbo Extra's, and was first tested in four store locations (Retailnews, 2019, par. 2). In January 2020, that number had increased to 50 stores, and one of Jumbo's directors confirmed that Jumbo intended to roll out the programme to all stores during the first half of 2020 (Pas, 2020, par. 2), most likely in February 2020 (Jumbo, 2020, FAQ question 6). The programme will be fine-tuned, but no major changes to its workings are expected before the major launch.

How it works

Every two weeks, a different collection of products give points when bought. There are certain brands that will give more points than others, and some categories or products are personalised, so not all customers get points when buying the same product (Jumbo, 2020, FAQ). There is an app in which customers can see which products will reward them with points. These points can be redeemed for free products or discounts on entrance to amusement parks or other entertainment.

The physical card and the app work alongside each other, although the card has to be activated or it will not allow saving points after 5 transactions without registration.

Jumbo Extra's can also be used to get a digital receipt, save other (discount) stamps digitally, and to set preferences regarding asking for savings stamps, receipts and other things at the register, to save the cashier and the customer time at checkout (Jumbo, 2020, FAQ).

The points are valid for two years, after which they will expire. This will take place every quarter.

Personal data

The Jumbo loyalty programme cannot be used anonymously; cards need to be registered in order to participate (Jumbo, 2020, FAQ).

When registering, customers need to fill in their first name, date of birth and email address. According to their FAQ, Jumbo uses the data of birth due to laws surrounding alcoholic products, the email address in order to send personalised points products and the first name 'to keep it personal'. Only in case the customer wants to use the same account to order groceries online and have them delivered to their house, it is necessary to provide the postal code and house number. Customers can also provide their preferred store location (Jumbo Extra's Algemene Voorwaarden, 2019).

Privacy notice

The Jumbo Extra's privacy statement is short and to the point. It is structured in the same way as the statements by Albert Heijn and Hema. Most points about data gathering, processing and changes or deletion of personal data are also described in the Frequently Asked Questions of the Jumbo Extra's programme. Jumbo, likely by accident, offers two slightly different Privacy Statements on their website, one from December 2019, accessible through the simulated Jumbo Extra's app; the other can be found as a direct link from the FAQ section

of the Jumbo Extra's website and dates to October 2019. In the section below, the most recent version will be used, except to outline some notable additions to the statement.

Usage of data. As stated before, Jumbo Extra's asks for the first name, date of birth and email address. For extra services, the customer can fill in their preferred store location, address, mobile phone number and family composition (in order to create more a more personalised range of products for collecting points) (Jumbo Extra's Privacy Statement, 2019b, p. 1).

The terms and conditions of the programme indicate Jumbo will combine the personal data with the customer's transaction data and search history on their website. This combined set of data will be used to make personal as well as generic analyses of the customer's purchasing behaviour and general purchasing behaviour of others, in order to offer personalised points products as well as "a better experience for our customers in the stores" (Jumbo Extra's Algemene Voorwaarden, 2019, p. 1-2).

The personal data the programme gathers, combined with the purchasing behaviour will be used to build a profile of customers, and by participating in the programme, the customer gives permission to Jumbo to profile them in this way. In the October version of the Jumbo Extra's Privacy Statement (2019a, p. 2), it is stated that only purchasing behaviour will be used to create a profile and for targeted marketing purposes. In the December version (Jumbo Extra's Privacy Statement, 2019b), this has changed to both the purchasing behaviour as well as any information gathered from the customer's participation in the loyalty programme.

The data from the loyalty programme will also be linked to the data gathered from visits to the Jumbo website, in case the user is registered to the website using the same account as for the Jumbo Extra's programme.

An interesting addition to the December version of the statement, is the introduction of Tokenisation. Jumbo is the only retailer of the three who mentions this in their privacy statement (Jumbo Extra's Privacy Statement, 2019b).

Tokenisation, according to Jumbo's definition, means they will link transactions that are made using the same bank card to each other. It states it will not use these transactions for targeted advertising or personalised discounts. However, if a customer has a Jumbo Extra's account and has used their bank card together with their Jumbo Extra's pass before, it will link the two together without the customer having to scan the card.

The privacy statement leaves the door open for Jumbo to link transactions that are made using the same bank card, even without a customer card. This would be unique; Jumbo states it will only use the data of loyalty programme customers to give personalised offers, but this

does not prevent them from using the data gathered using tokenisation in an aggregated manner to do purchasing behaviour analyses.

Third parties with access to data. Jumbo states it will share personal data with third parties only when necessary for the execution of the programme: in this case, email communication, sending push notifications and analysing the purchasing behaviour to offer personalised discounts and offers. It does not specify this point further (Jumbo Extra's Privacy Statement, 2019b).

Protection of data. Of the three retailers studied, Jumbo has the shortest paragraph concerning the protection of data. It merely states that good data protection if valuable to Jumbo and it uses appropriate technical and operational measures to prevent information from getting damaged, lost or corrupted (Jumbo Extra's Privacy Statement, 2019b).

Conclusion

Jumbo is only just starting out with its loyalty programme. It asks for very little in terms of personal data; much less than the other two retailers. Although their programme has not had the time to develop as much as the others, it is clear that Jumbo is taking the gathering of customer data seriously. Contrary to the other retailers, it mentions the use of tokenisation in order to link purchases to the same individual/bank card. This might allow Jumbo to link transactions together without needing a loyalty card, which could potentially greatly increase the amount of data it can use to do aggregated analyses.

7. Analysis: shaping the matrix

This chapter will aim to combine use various sources to set out requirements and find out what other measures retailers with loyalty programmes are taking and what they run into in practice. It is separated into three categories: one related to technological measures, one related to organisational measures, and one related to anything on the customer-side. These categories will be discussed separately.

The matrix takes its data from the requirements, set out in chapter 5, the case studies, set out in chapter 6, as well as data from interviews (Appendix 1). The interviews took place with three different retailers with loyalty programmes; these are not necessarily the same retailers as the case studies. The interviews were conducted on the basis of anonymity for the organisations, preventing identification of what measures were taken by what retailers. As companies only cooperated with interviews anonymously, this disallowed a combination of 'behind the scenes' info with publicly available information found in the case studies.

This chapter aims to answer the sub-questions "what actions are retailers taking (or planning to take) to meet the recommended security requirements regarding data protection?" and "what difficulties are companies experiencing in their efforts towards adequate personal data protection?".

Technology

The requirements in the technology column were built up using the ISO 27001/27002/27701 security standards and article 32 of the GDPR. This combination informed the requirements as set out in the relevant chapter. Six of these included technical measures: requirements 1 through 6.

Interviews with retailers about their data protection revealed that the retailers outsource a large part of their information security (Appendix 1, transcr. 1, q. 3; transcr. 2, q. 5; transcr. 3, q. 5). For this reason, most of the technical measures could not be verified in the interviews. It must be assumed that the standards or guidelines used by all organisations (see discussion of requirements 7 and 11 below) mean that the necessary technological measures set out in requirements 1 through 6 are implemented. One requirement that was explicitly stated to be in use was requirement 1: pseudonymisation. One retailer used a 'privacy locker' through which all personal data must go in order to encrypt it, before it is able to be used for analyses (Appendix 1, transcr. 2, q. 8).

Requirements 5 and 6 (other technical measures and data breach protection) are in both the technology and the organisation column, as they include measures that can be both technical and operational.

These requirements form the following table:

TECHNOLOGY

REQ 1	Pseudonymisation & encryption
REQ 2	Maintaining confidentiality, integrity, availability, access
REQ 3	Resilience of processing systems and services / backups
REQ 4	Regular evaluations and testing
REQ 5	Other technical measures
REQ 6	Data breach protection

Table 2. Technology column.

Organisation

It is not enough for an organisation to have a completely technically secure IT environment if its users are not qualified to use it. Thus, the basis for the secure use of databases includes both secure technical functioning as well as adequate operational controls. As Von Solms (1999, p. 53) puts it: "[…] a motor vehicle with all the required technical safety mechanisms, may be driven in a very reckless manner by its driver. Therefore, the driver needs to be in possession of a valid driver's license to ensure that all the technical safety features are used correctly. Technical security mechanisms need to be augmented by proper operational procedures in order to be effective".

This section deals with operational or organisational measures to be carried out in order to meet recommended security standards regarding (personal) data protection. This column includes five requirements set out in chapter 5: requirements 5 through 9.

Interviews with three retail companies showed all organisations were very data driven (Appendix 1, transcr. 1, q. 2; transcr. 2, q. 3; transcr. 3; q. 3). The data from the loyalty programmes is used in many aspects of the decision making throughout the organisations. This necessitates a culture of information security awareness throughout the whole company, as the data is spread throughout the organisation. This fits with requirement 9, or REQ9 in the matrix. The fact that security awareness is important to retailers can also be deduced from the fact that they hire external parties to help them spread security awareness throughout the organisation,

or have themed weeks in which the importance of data and data protection are stressed (Appendix 1, transcr. 2, q. 5, 9).

Other requirements were confirmed to be used in practice in the interviews as well, such as requirement 8: how to act as a controller of personal data (Appendix 1, transcr. 1, q. 3).

From the case studies, it was gathered that the companies differ in the way in which the personal data from the loyalty programmes is used. However, one thing in common is that they all use it to build customer segments, groups or profiles in order to 'make sense' of their customer base. Of the three, Albert Heijn seems most elaborate when it comes to building customer profiles. It keeps a comprehensive database that includes data from various third party sources to create customer segments.

In the case studies, it became clear that all three retailers generally analyse purchasing behaviour in an aggregated way, using these segmentation or profiling methods. This will be added to the matrix as REQ10: segmentation/profiling of customer groups.

Requirement 7 deals with certification; how "[adhering] to a code of conduct or an internationally recognised certification body is recommended to demonstrate compliance with all security regulations and keep data as safe as possible" (see chapter 5). From the interviews, an extra dimension must be added to this. In order to become certified, adherence to strict models or standards is required. This does not always fit the corporate culture of an organisation.

The three interviewed companies used different strategies. None of the companies was ISO-certified. One of them used comprehensive information security standards to inform its security (Appendix 1, transcr. 2, q. 6), while two others used frameworks based on international security frameworks, but translated into terms or guidelines that fit the organisation, as it was felt that having the rigid models of the ISO standards would impede entrepreneurialism and did not fit the companies' culture (Appendix 1, transcr. 1, q. 5, transcr. 3, q. 6). This will be added to the matrix as REQ11: adapting guidelines to fit the corporate culture.

These requirements form Table 3, seen on the next page.

ORGANISATION

REQ 5	Other operational measures
REQ 6	Data breach protection
REQ 7	Certification
REQ 8	Controller instructions
REQ 9	Security awareness internally
REQ 10	Segmentation/profiling of customer groups
REQ 11	Adapting guidelines to fit corporate culture

Table 3. Organisation column.

Customer

The third column deals with the customer side, anything related to (personal) data protection externally, not internally.

From the case studies, it was gathered the three differ in how open they are about what they do with the loyalty programme data, who they work with and how they aim to protect it.

Albert Heijn is very open about how it uses the data, who the third parties they work with are and what they do, and they are (relatively) open about what measures they have taken to ensure adequate data protection.

Hema does not communicate extensively about how they protect the data or who they work with, but they are clear in how they use their data and present is accessibly. Jumbo is similar to Hema in this aspect, although they are more open about what they do with the data upfront, and do not ask for a lot of personal data.

Being transparent about the usage and the protection of personal data as well as the third parties the companies work with related to personal data are three requirements that will be added to the matrix, as Requirements 12, 13 and 14, respectively.

In one of the interviews, the necessity to be careful with personalisation was mentioned. If personalisation goes too far or in a wrong direction, the customer might be put off or develop negative feelings towards the company or towards the loyalty card. An example given in one of the interviews was that of someone without children, who might get advertisements for baby products because she fit into the right age category (Appendix 1, transcr. 1, q. 11). Blowback to this profiling was also felt by Albert Heijn when the profiles it used to inform its employees became public in 2018, and were consequently widely criticised; as mentioned in the case study.

This shows the downsides to profiling; if it goes wrong, the customer is at best likely not to get relevant discounts, and at worst feels put off by the store. This will be included in the matrix as REQ 15: wariness about profiling and personalisation.

Customer trust was brought up as a reason to be hesitant about asking too much personal data and as an argument in favour of strict data protection policies (Appendix 1, transcr. 2, q. 8; transcr. 3, q. 6). In an interview, one brand indicated it valued its reputation as a trustworthy, reliable brand, and had guidelines in place that were stricter than legally necessary. Another brand had had a close call with the privacy authority due to a shortcoming in the cookie-consent form, and was happy when they were able to resolve the problem without it becoming public and without a large fine. The PR aspect of the necessity of data protection will be added to the matrix as REQ 16: mitigating potential reputation damage through adequate data protection.

Combining these requirements leads to the following table:

	CUSTOMER
REQ 12	Transparency about usage of data
REQ 13	Transparency about protection of data
REQ 14	Transparency about third parties
REQ 15	Wariness about profiling and personalisation
REQ 16	Mitigating potential reputation damage through adequate data protection

Table 4. Customer column.

The matrix

The combination of these three columns give us the full matrix of recommended measures and guidelines to ensure adequate data protection, see Table 5 below:

	TECHNOLOGY		**ORGANISATION**		**CUSTOMER**
REQ 1	Pseudonymisation & encryption	*REQ 5*	Other operational measures	*REQ 12*	Transparency about usage of data
REQ 2	Maintaining confidentiality, integrity, availability, access	*REQ 6*	Data breach protection	*REQ 13*	Transparency about protection of data
REQ 3	Resilience of processing systems and services / backups	*REQ 7*	Certification	*REQ 14*	Transparency about third parties
REQ 4	Regular evaluations and testing	*REQ 8*	Controller instructions	*REQ 15*	Wariness about profiling and personalisation
REQ 5	Other technical measures	*REQ 9*	Security awareness internally	*REQ 16*	Mitigating potential reputation damage through adequate data protection
REQ 6	Data breach protection	*REQ 10*	Segmentation/profiling of customer groups		
		REQ 11	Adapting guidelines to fit corporate culture		

Table 5. The final matrix.

8. Conclusion

This thesis was guided by the research question "to what extent have offline retailers with loyalty programmes taken action to comply with GDPR's data protection requirements and international information security standards?".

In order to form an answer to the main research question, three sub-research questions were looked at. The first sub-question was to find out which security requirements can be identified using article 32 of the GDPR and ISO security standards. Article 32 of the GDPR was analysed, combined with control variables found in security standards ISO27001, ISO27002 and ISO27701. These together were used to formulate nine requirements for adequate personal data protection, of which 6 were mostly technical measures. These measures included pseudonymisation, measures to maintain confidentiality, integrity availability and access to personal data, regular evaluations of security protocols and others.

Not all of these requirements could be verified through interviews at different retailers, as they were unable or unwilling to answer questions regarding specific technical measures. However, the interviews did confirm most of the technical requirements to be in use at the interviewed companies.

This leads to the second sub-question: "what actions are retailers taking (or planning to take) to meet the recommended security requirements regarding data protection?". Besides confirmation that what was found in the GDPR/ISO standards analysis generally holds up in practice, the case studies and the interviews lead to the conclusion that there are more requirements to having adequate personal data protection related to loyalty programmes.

The retailers mostly refrain from using customers' individual personal data; it uses customer groups (aggregated datasets) to do analyses on purchasing behaviour or customer habits. In the case studies, an analysis of the privacy statements and public information released by the retailers showed that all retailers are using the data gathered from the loyalty programmes to create profiles or segments of customers. These groups are used to better tailor discounts or communication to customers. Before customers are grouped, their personal data is usually hashed, making it untraceable to an individual consumer.

Another learning from the case studies was the fact that transparency about the usage of personal data, protection of that data and the involvement of third parties in the processing of personal data differs greatly per retailer. Some retailers are very transparent; others keep their explanations very brief. By being open and transparent about what and how personal data is used, retailers can be ahead of the curve and show they take their responsibility in the usage and protection of personal data seriously.

This transparency might also have drawbacks, which are addressed in the answers to the last sub-question, “what difficulties are companies experiencing in their efforts towards adequate personal data protection?” Based on the interviews, it was found that retailers had to do extensive privacy assessments within their organisations to ensure they were GDPR-compliant in the implementation period, and some had to change their ways in order to become compliant. Certain companies have run into problems with privacy authorities, or have had to stop doing certain analyses with personal data because they would not be compliant with the privacy regulation.

Other difficulties companies ran into included possible negative publicity from the profiling that is done on the basis of their customer data, if it comes out. This happened to Albert Heijn in 2018, for instance. Another retailer indicated in an interview that they were very hesitant with their usage of personal data, specifically to prevent any PR scandals that would damage their brand.

There is no single answer to the main research question, to what extent offline retailers with loyalty programmes have taken action to comply with GDPR’s data protection requirements and international information security standards. From the case studies and the interviews, it appeared that retailers take their roles in the protection of personal data from loyalty programmes seriously. The data that is gathered through the programmes is very valuable to the retailers, and they are glad to take the opportunity to use the data to the highest extent. However, most are doing what they can to protect the data, using international standards and internal guidelines to guide their organisations towards adequate data protection. Seeing as the data of the customer cards is used extensively, and throughout the organisations, security awareness throughout the company remains a priority for the interviewed retailers. While there is room for improvement in how some retailers communicate what they are doing with the personal data or who they are working with, most realise customers value their privacy and are trusting the company to handle their data carefully. The companies feel pressure to have adequate data protection, not solely because of their legal obligations, but also due to PR pressure when a security incident becomes public.

Online retailers are generally having an easier time gathering data on their customers, as it is easier to link online orders to an individual. Offline retailers traditionally had more difficulty linking different transactions to the same customer, making analyses of purchasing behaviour difficult.

However, loyalty programmes allow retailers to link transactions and conduct these analyses, making them an invaluable source of data. Before, there had not been a lot of research

done on the topic of (personal) data protection by offline retailers. As retailers are doing more and more analyses and gathering more and more data (through their loyalty programmes), this paper sought to find out how seriously offline retailers are taking their obligations in the protection of their data. By doing an examination of what retailers should be doing and what they are doing, this knowledge gap was closed a bit more.

This thesis had some limitations. For instance, most offline retailers, including the ones discussed in this paper, combine their online and offline retail activities, meaning they might already have data on their customers from their websites or apps. Thus, it cannot be said that this research looks solely at the loyalty programmes of offline retailers, as the retailers use the data from both online and offline for their analyses. Their data protection practices most likely do not differ for either sets of data.

A major impediment to this research was the fact that it was impossible to link data gathered from interviews, the 'behind the scenes' knowledge, to the data gathered from case studies. Companies were only willing to cooperate with interviews on the basis of anonymity, preventing case studies from being matched with interview data and preventing strong conclusions. The original intent of this research was to use the matrix to examine how the matrix matches up with practices at retailers. However, not being able to link internal, organisational or technical data with publicly available data blocked that avenue of the research.

Furthermore, this research only looked at one article of the GDPR. In future research, it is recommended to look at more than just article 32, in order to form a complete picture of the information security of retailers. It is also wise to include more of the control variables of the ISO standards, and to involve other international security standards as well.

The author did not have access to the original security standards, meaning all information on them had to be gathered from sources describing them. As the ISO27701 standard came out while this thesis was already being written, it was not fully incorporated in the analysis, as little secondary literature could be found on it.

Additionally, this research only looked into three retailers, and those three were all major players in their field. In future research, it is worth looking into whether this created a bias, as these large organisations might have an advantage over smaller companies due to their size. Two of the three retailers were active in the same branch (supermarkets), which might also paint a distorted picture. It is recommended to diversify both the case studies and the interviews with retailers in order to get a better perspective of data protection in the field of offline retail.

References

Albert Heijn Bonuskaart (n.d.). *Bonuskaart.* Retrieved January 2020 from https://www.ah.nl/bonuskaart/

Albert Heijn Privacybeleid (2020, January 23). *Privacybeleid van Albert Heijn B.V.* Retrieved January 2020 from https://www.ah.nl/privacy/

Allport, M. (2019, January 30). ISO 27001 vs Cobit 2019. *Compliance Council*. https://blog.compliancecouncil.com.au/blog/iso-27001-vs-cobit-2019

Autoriteit Persoonsgegevens (AP). (2019). Grip op persoonsgegevens: Jaarverslag 2018. *Autoriteit Persoonsgegevens.* Retrieved from https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2018.pdf

Autoriteit Persoonsgegevens (AP). (2019). *Ontwerpbesluit AP gedragscode Nederland ICT*. Autoriteit Persoonsgegevens. Retrieved from https://autoriteitpersoonsgegevens.nl/nl/nieuws/ontwerpbesluit-ap-gedragscode-nederland-ict

Bird, K. (2013, October 4). *Are you prepared for information security breaches? New ISO/IEC 27001 can help*. ISO. Retrieved from ISO website: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/2013/10/Ref1783.html

Bouca, C. (2016, October 16). *EU GDPR: Does ISO 27001 implementation satisfy its requirements?* 27001Academy. Retrieved from https://advisera.com/27001academy/blog/2016/10/17/does-iso-27001-implementation-satisfy-eu-gdpr-requirements/

Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report*, *11*(1), 26–31. https://doi.org/10.1016/j.istr.2005.12.001

Bryman, A. (2016). *Social research methods*. Oxford University Press.

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Rao, H. R. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems*, *83*, 47-56.

Consumentenbond. (2013, September 26). *AH bonuskaart zo lek als een mandje*. Consumentenbond. https://www.consumentenbond.nl/nieuws/2013/ah-bonuskaart-zo-lek-als-een-mandje

Cooper, T., & LaSalle, R. (2016). *Guarding and growing personal data value*. Retrieved from https://www.accenture.com/t20180306t084026z__w__/us-en/_acnmedia/pdf-32/accenture-guarding-and-growing-personal-data-value-pov-low-res.pdfla=en

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

Data Guidance. (2019, July 24). ISO 27001—Information Security Management System. *OneTrust*. Retrieved from DataGuidance website: https://free.dataguidance.com/laws/iso-iec-270012013/

Deibel, M., Eppinga, S., & Goethem, K. (2015, January 3). Een kaart vol met "big data." *NRC Handelsblad*. Retrieved from https://www.nrc.nl/nieuws/2015/01/03/een-kaart-vol-met-big-data-1452795-a1264242

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2019). GDPR and ISO/IEC 27001: Synergies of Activities Towards Organisations' Compliance. *International Conference on Trust and Privacy in Digital Business*, 94-109.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *04*(02), 92–100. https://doi.org/10.4236/jis.2013.42011

Distrifood. (2017, January 9). Hema komt met eigen klantenkaart. *Distrifood*. Retrieved from https://www.distrifood.nl/formules/nieuws/2017/01/hema-komt-met-eigen-klantenkaart-101104418

Emerce. (2013, October 8). Nieuwe bonuskaart Albert Heijn kan online worden geactiveerd. *Emerce blog*. Retrieved from https://www.emerce.nl/nieuws/nieuwe-bonuskaart-albert-heijn-kan-online-worden-geactiveerd

Etos. (2019, September 11). *Privacybeleid Etos*. Retrieved from https://www.etos.nl/privacybeleid.html

European Data Protection Supervisor (EDPS). (2016, December 13). Overview of Definitions; Glossary: P. Retrieved from European Data Protection Supervisor website: https://edps.europa.eu/data-protection/data-protection/glossary/p_en

Feiereisen, S. (2019, April 8). 18 retailers with the best loyalty programs. Retrieved 4 October 2019, from Business Insider Nederland website: https://www.businessinsider.com/best-loyalty-programs-stores-2019-4

Fomin, V. V., Vries, H., & Barlette, Y. (2008, September). ISO/IEC 27001 information systems security management standard: exploring the reasons for low adoption. In *EUROMOT 2008 Conference, Nice, France*.

Garstenveld, P. (2019, April 4). *Jumbo werkt aan een kortingssysteem voor trouwe klanten.* Distrifood. https://www.distrifood.nl/formules/nieuws/2019/04/jumbo-werkt-aan-een-kortingssysteem-voor-trouwe-klanten-101123232

GDPR Register. (2018, October 5). *Loyalty Programs Under the Radar of GDPR.* Retrieved from GDPR Register website: https://www.gdprregister.eu/gdpr/loyalty-programs-under-gdpr/

General Data Protection Regulation (GDPR). (2016). *European Union Parliament General Data Protection Regulation*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504

Gómez, B. G., Arranz, A. M. G., & Cillán, J. G. (2012). Drivers of customer likelihood to join grocery retail loyalty programs. An analysis of reward programs and loyalty cards. *Journal of Retailing and Consumer Services*, *19*(5), 492-500.

Goslinga, R. (2017, September 14). *Ceo Tjeerd Jegen over de metamorfose van Hema*. Management Scope. Retrieved from https://managementscope.nl/magazine/artikel/1078-metamorfose-hema

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175.

Heilbron, B., & Koopman, E. (2019, January 16). De Autoriteit Persoonsgegevens is altijd klein en tandeloos gehouden. *De Groene Amsterdammer*. Retrieved from https://www.groene.nl/artikel/de-tragedie-van-het-privacytoezicht

Hema (2017). Algemene voorwaarden. Retrieved from https://www.hema.nl/on/demandware.static/-/Library-Sites-HemaContentLibrary/nl_NL/pdf/HEMA-algemene-voorwaarden-NL.pdf

Hema (2019). *Privacy Statement*. Hema website. Retrieved from https://www.hema.nl/privacy-statement

Hema (n.d.). *Meer Hema klantenpas*. Hema website. Retrieved from https://www.hema.nl/meerhema

Henderson, C. M., Beck, J. T., & Palmatier, R. W. (2011). Review of the theoretical underpinnings of loyalty programs. *Journal of Consumer Psychology*, *21*(3), 256–276. https://doi.org/10.1016/j.jcps.2011.02.007

HeyHema (2019, September 5). Jij vraagt, meer HEMA antwoordt: meer over de leukste klantenpas van Nederland! *HeyHema intranet*. Retrieved from https://heyhema.com/

Hill, K. (2012, February 16). How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. *Forbes*. Retrieved from www.forbes.com

Höne, K., & Eloff, J. H. P. (2002). Information security policy—What do international information security standards say? *Computers & Security*, *21*(5), 402–409. https://doi.org/10.1016/S0167-4048(02)00504-7

Humphreys, E. (2006). State-of-the-art information security management systems with ISO/IEC 27001: 2005. *ISO Management Systems*, *6*(1).

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, *13*(4), 247–255. https://doi.org/10.1016/j.istr.2008.10.010

ICO - Information Commissioner's Office UK. (2019). *Guide to the General Data Protection Regulation (GDPR).* Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Imperva. (2019). GDPR Article 32. *Imperva: Data Security, Regulation & Compliance*. Retrieved from https://www.imperva.com/learn/data-security/gdpr-article-32/

Irwin, L. (2019, February 7). *Securing 2019 with ISO 27001*. IT Governance Blog. Retrieved from https://www.itgovernance.eu/blog/en/securing-2019-with-iso-27001

ISF. (2018). *The ISF Standard of Good Practice for Information Security 2018*. Information Security Forum. https://www.securityforum.org/tool/the-isf-standard-good-practice-information-security-2018/

ISO & CERN. (2014). Standardization and Innovation. *ISO-CERN Conference Proceedings November 2014.* Retrieved from https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/standardization_and_innovation.pdf

ISO. (2019). ISO Annual Report 2018: Advancing the global agenda. Retrieved from https://www.iso.org/files/live/sites/isoorg/files/about%20ISO/annual_reports/en/annual_report_2018_en.pdf

ISO/IEC 27001. (2013). *Information technology – information security management systems requirements.* Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

IT Governance Europe. (2018, August 30). ISO 27001 Global Report 2018. Retrieved from https://www.itgovernance.co.uk/iso27001-global-report-2018

IT Governance Europe. (2019a). ISO 27001: The Facts. Retrieved from https://www.itgovernance.eu/en-ie/iso27001-factsheet-ie

IT Governance Europe. (2019b, September). ISO 27701 Privacy information management systems. Retrieved from https://www.itgovernance.eu/en-ie/iso-27701-pims-thank-you-ie

Jansen, R. (2018, July 12). *Jumbo test sparen voor kassakorting*. Distrifood. https://www.distrifood.nl/branche-bedrijf/nieuws/2018/07/jumbo-test-sparen-voor-kassakorting-101118102

Jumbo (2020). *Jumbo Extra's*. Jumbo website. Retrieved from https://www.jumbo.com/service/jumbo-extras

Jumbo Extra's Algemene Voorwaarden. (2019, December 19). *Jumbo Extra's Algemene Voorwaarden*. Retrieved from: https://www.jumbo.com/dam/service/jumbo-extra/Jumbo-Extras-AlgemeneVoorwaarden.pdf

Jumbo Extra's Privacy Statement. (2019a, October 1). *Jumbo Extra's Privacy Statement.* Retrieved from https://www.jumbo.com/dam/service/jumbo-extra/Jumbo-Extras-Privacystatement.pdf

Jumbo Extra's Privacy Statement. (2019b, December 19). *Jumbo Extra's Privacy Statement*. Retrieved from https://www.jumbo.com/extras/app

Kamenjasevic, E. (2018, September 18). *Compliance certification scheme under the GDPR*. KU Leuven: CITIP Blog. Retrieved from https://www.law.kuleuven.be/citip/blog/compliance-certification-scheme-under-the-gdpr/

Karyda, M., & Mitrou, L. (2016). *Data Breach Notification: Issues and Challenges for Security Management.* MCIS.

Kreiken, F. (2016a, February 4). Transparent Consumers: data brokers and profiling in the Netherlands. *Bits of Freedom.* Retrieved from https://www.bitsoffreedom.nl/wp-content/uploads/transparent-consumers%E2%80%94bits-of-freedom.pdf

Kreiken, F. (2016b, March 9). Houden datahandelaren zich aan de wet?. *Bits of Freedom*. Retrieved from https://www.bitsoffreedom.nl/2016/03/09/houden-datahandelaren-zich-aan-de-wet/

Lakshmanan, R. (2019, June 12). Loyalty programs cost you your personal data—Are the rewards worth it? Retrieved from The Next Web website: https://thenextweb.com/insights/2019/06/12/loyalty-programs-cost-you-your-personal-data-are-the-rewards-worth-it/

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36-58.

Mast, J. (2018, October 25). Sparen met een klantenkaart, lucratief of niet? *PlusOnline*. Retrieved from https://www.plusonline.nl/sparen/sparen-met-een-klantenkaart-lucratief-of-niet

Naden, C. (2019, August 6). *Tackling privacy information management head on: First International Standard just published*. ISO. Retrieved from ISO website: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/2019/08/Ref2419.html

NDC. (2018, April 6). *GDPR and ISO 27001—A winning combination for compliance*. Retrieved from NDC Global Auditors website: https://www.ndcmanagement.co.uk/blog/gdpr-and-iso-27001/

NEN. (2019). *ISO/IEC 27701:2019 EN*. Retrieved from https://www.nen.nl/NEN-Shop/Norm/ISOIEC-277012019-en.htm

NQA. (2019). *ISO 27701: GDPR Compliance Management System*. Retrieved from https://www.nqa.com/nl-nl/certification/standards/iso-27701

Nunes, J. C., & Drèze, X. (2006). Your Loyalty Program Is Betraying You. *Harvard Business Review*, 9.

Oosterhout, A. (2017, June 21). Hema maakt er meer van. *Twinkle*. Retrieved from https://twinklemagazine.nl/2017/06/hema-maakt-er-meer-van/index.xml

Pas, H. (2020, January 30). *Jumbo zet gas op Extra's en Foodcoach.* Distrifood. https://www.distrifood.nl/formules/nieuws/2020/01/jumbo-zet-gas-op-extras-en-foodcoach

Privacy First. (2013, October 4). Zorgen over privacy AH Bonuskaart. *Privacy First blog*. https://www.privacyfirst.nl/in-de-media/item/677-eenvandaag-26-september-2013-zorgen-over-privacy-ah-bonuskaart.html

Retailnews. (2014a, April 23). *"Albert Heijn koppelt bonuskaarten."* RetailNews. Retrieved from https://retailtrends.nl/news/36354/albert-heijn-koppelt-bonuskaarten

Retailnews. (2014b, September 23). *AH investeert in online voor persoonlijke relatie*. RetailNews. Retrieved from https://retailtrends.nl/news/37825/ah-investeert-in-online-voor-persoonlijke-relatie

Retailnews. (2019, December 19). *Jumbo rolt spaarprogramma Extra's verder uit*. RetailNews. https://retailtrends.nl/news/58764/jumbo-rolt-spaarprogramma-extras-verder-uit

Retailnews. (2020, January 30). Kruidvat blijft verreweg de grootste retailer. *RetailNews*. Retrieved from https://retailtrends.nl/news/59300/kruidvat-blijft-verreweg-de-grootste-retailer

Rhoen, M. H. C. (2019). *Big data, big risks, big power shifts: Evaluating the General Data Protection Regulation as an instrument of risk control and power redistribution in the context of big data* [Leiden University]. https://openaccess.leidenuniv.nl/handle/1887/77748

Rhoen, M. H. C. (2020, February 2). *De AVG houdt big data onvoldoende in bedwang*. Netkwesties. https://www.netkwesties.nl/1420/de-avg-houdt-big-data-onvoldoende-in.htm

Rosen, P. (2019, May 15). Legal Landmines And Patchworks: The State Of Privacy And Cybersecurity Compliance For Business. *Forbes.* Retrieved from www.forbes.com

RTL Nieuws (2018, February 12). Al twintig jaar korting! De bonuskaart is jarig. *Editie NL*. Retrieved from https://www.rtlnieuws.nl/editienl/artikel/3852726/al-twintig-jaar-korting-de-bonuskaart-jarig

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), 202-209.

Schrameyer, H. (2019, September 12). *Jumbo komt met digitaal loyaliteitsprogramma*. MarketingTribune. https://www.marketingtribune.nl/food-en-retail/nieuws/2019/09/jumbo-komt-met-digitaal-loyaliteitsprogramma/index.xml

Schroeder, D. (2019). *ISO 27001 Offers Data Processors a Roadmap to GDPR 'Sufficient Guarantees'*. Retrieved from Aprio website: https://www.aprio.com/whatsnext/iso-27001-offers-data-processors-roadmap-gdpr-sufficient-guarantees/

Scroxton, A. (2019, September 11). GDPR non-compliance worse than feared. *Computer Weekly*. Retrieved from: https://www.computerweekly.com/news/252470436/GDPR-non-compliance-worse-than-feared

Staalduine, J. (2018, January 13). Albert Heijn leert medewerkers dat "budgetklant" donker is en kroeshaar heeft. *De Volkskrant*. https://www.volkskrant.nl/economie/albert-heijn-leert-medewerkers-dat-budgetklant-donker-is-en-kroeshaar-heeft~b5a7ba53/

Stebbins, R. A. (2001). *Exploratory research in the social sciences* (Vol. 48). Sage.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). *Information Security Management System Standards: A Comparative Study of the Big Five*. *11*(05), 7.

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, *2016*(6), 5-8.

Tene, O., & Polonetsky, J. (2011). Privacy in the Age of Big Data: A Time for Big Decisions Symposium Issue: The Privacy Paradox: Privacy and Its Conflicting Values. *Stanford Law Review Online*, 63–69.

Terra, C. (2018, January 4). 3 miljoen leden voor 'Meer Hema'-klantenpas, 'uitrol buitenland in 2019'. *Fashion United*. Retrieved from https://fashionunited.nl/nieuws/retail/3-miljoen-leden-voor-meer-hema-klantenpas-uitrol-buitenland-in-2019/2018010430493

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134-153.

Toonen, L. (2017, May 18). Het loyaliteitsprogramma van ons allemaal. *LoyaltyFacts*. Retrieved from https://www.loyaltyfacts.nl/interview/het-loyaliteitsprogramma-van-ons-allemaal/

Verhoef, P. C., Kannan, P. K., & Inman, J. J. (2015). From multi-channel retailing to omni-channel retailing: introduction to the special issue on multi-channel retailing. *Journal of retailing*, *91*(2), 174-181.

Vermeulen, S. (2018). *Hema: de onwaarschijnlijke ontsnapping van een nationaal icoon*. Prometheus.

Verschuren, P., Doorewaard, H., & Mellion, M. (2010). *Designing a research project* (Vol. 2). The Hague: Eleven International Publishing.

Vlems, E. (2014, April 25). *Ik wil geen aanbiedingen meer van de Jumbo*. Marketingfacts. https://www.marketingfacts.nl/berichten/ik-wil-geen-aanbiedingen-meer-van-de-jumbo

von Solms, R. (1999). Information security management: Why standards are important. *Information Management & Computer Security*, *7*(1), 50–58. https://doi.org/10.1108/09685229910255223

Voorn, H. (2017, July 12). HEMA: "Dit jaar gepersonaliseerde communicatie, daarna volgt het aanbod." *Emerce*. https://www.emerce.nl/interviews/hema-dit-jaar-gepersonaliseerde-communicatie-daarna-volgt-aanbod

Vreeling, R. J. (2018, September 6). *Het verschil tussen ISO 27001 en 27002, hoe zit dat?* Retrieved from CertificeringsAdvies Nederland website: https://certificeringsadvies.nl/het-verschil-tussen-iso-27001-en-27002-hoe-zit-dat/

Wierenga, M. (2019, July 2). *Digital marketing in 2019: Datagedreven personaliseren en usability op één*. Marketingfacts. Retrieved from

https://www.marketingfacts.nl/berichten/digital-marketing-live-2019-datagedreven-personaliseren-usability-op-een

Zerlang, J. (2017). GDPR: A milestone in convergence for cyber-security and compliance. *Network Security*, *2017*(6), 8–11. https://doi.org/10.1016/S1353-4858(17)30060-0