UCD Michael Smurfit
Graduate Business School

MSc. Management

Group Project (2017-2018)– ICT Strategy

Business Information Systems Management

(MIS40760)

Name	**Student Number**	**Email**
Aaruni Bhugul	17200419	aaruni.bhugul@ucdconnect.ie
Ankita	17204239	ankita@ucdconnect.ie
Chinmay Kuchya	17201526	chinmay.kuchya@ucdconnect.ie
Prashik Vijay Chitkesiwar	17200040	prashik.chitkesiwar@ucdconnect.ie
Samuel Sherin Varghese	17200643	samuel.varghese@ucdconnect.ie

Table of Contents

1. Introduction to GDPR

Internet is governed by the existence of handful of meaningful laws. Cyberspace is an ever-evolving area which caters to criminality, and illegal & outrageous behaviour. No set of laws can change practices compromising cyberspace security, on the other hand it will be unethical and unlawful, if no strict measures are taken. Failure to adapt according to changing environment will lead to nations plummeting down the cyber curve.

In the 1990s, the laws overseeing how individuals' information ought to be managed were drawn up but with the passing years, a great deal of it has been changed. We now make immense amounts of computerized data every day and everything from cell phones to smart watches gather information that could recognize our existence.

General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). GDPR sets out the principles for data management and rights of the individual and imposes revenue-based fines. The General Data Protection Regulation covers all companies that deal with data of EU citizens. GDPR will come into effect across the EU on May 25, 2018 (Beattie, 2018).

Even though a company is not based in EU region, it will have to comply with GDPR in case of collection of data in any form of any EU citizen. Non-compliance to upcoming GDPR will lead to hefty fine, up to 4% of the annual revenue of the firm.

1.1. What is personal data?

The EU has significantly extended the meaning of individual information under the GDPR. To mirror the kinds of information associations now gather about individuals, online identifiers, for example, IP tends to now qualify as individual personal information. Other data such as financial, social or emotional wellness data, are also taken as identifiable data**.** (Curtis,2018)

These incorporate exchange union membership, religious convictions, political conclusions, racial data, and sexual orientation are considered as sensitive personal data.

1.2. Principle factors behind the presentation of GDPR

The main factor is the EU wants to align data protection law with how an individual's information is being utilized, particularly considering organizations like Amazon, Google, Twitter, and Facebook, who offer their administrations for no cost thereby taking all the personal individual data. One of the best examples of these threats of giving such immense authorizations can be outlined by the continuous Cambridge Analytica outrage, where 50 million Facebook profiles were reaped to impact the 2016 US election.

The second reason is giving better clarity to organizations over the legitimate condition that directs how they can carry on their business. By making data protection law indistinguishable throughout all member countries, the EU trusts this will save all organizations €2.3 billion yearly **(**Curtis, 2018).

All the reforms going into effect are designed to help customers gain a greater level of control over their data, while offering more transparency throughout the data collection and use process. These new laws will help in bringing existing legislation up to par with the connected digital age we live in. Since data collection is such a normal and integral aspect of our lives both on a personal and business level it helps to set the standard for data-related laws moving forward.

Data Protection laws manages the exchanges of making, sparing, sharing of individual's personal details. These days creating individual profile is exceptionally basic in this computerized period whether it's for shopping or socializing with others or wherever, sharing details online has now become compulsory for making profile. These profiles save individual subtle elements which ought to be private and then these personal details are imparted to outsider party. Incongruity is that individuals accept these terms by a single tick without perusing the terms and conditions which prompts sharing of the individual personal details to outsider lawfully. For the information assurance these sorts of practices are challenging where individual concurred the terms and conditions without knowing it. Data protection is the request of advanced age in which we are managing gathering of information, access of information, breaking down of information and utilization of information in different routes by different organizations.

1.3. Steps Required for GDPR Compliant

1. Awareness

The decision makers and individuals in the organization should be aware that the law is changing to the GDPR. They must value its effect and recognize areas that could cause consistent issues under the GDPR. It is helpful to begin by taking a gander at your association's risk register. Executing the GDPR could have huge asset suggestions, particularly for bigger and more mind-boggling associations (Ico.org.uk, 2018).

2. Timely breach notification

Under the GDPR, breach warning will become necessary in all parts of EU where a data breach is probably going to result in a hazard for the rights and flexibilities of people. This must be done within 72 hours of first having realized of the breach. Data processors will likewise be required to advise their clients, the controllers immediately after first getting to be mindful of a data breach (Xcoobee.com, 2018).

3. Right to data access

Right to access illustrated by the GDPR is the right for data subjects to acquire from the data controller affirmation with respect to regardless of whether personal information concerning them is being prepared, where and for what reason. Further, the controller should give a duplicate of the individual data for free, in an electronic configuration. This change is a sensational move to information transparency and strengthening of information subjects (Burgess, 2018).

4. *Right to be forgotten*

People additionally have the privilege to request that their information is erased if it's never again important to the reason for which it was gathered. This is known as the 'right to be forgotten'. Under this right, they can likewise request that their information is eradicated if they've pulled back their consent for their information to be gathered or question the way it is being handled (Curtis, 2018).

5. *Data portability*

GDPR presents data portability which is the right for an information subject to get the individual information concerning them and is carried out by automated means and have the privilege to transmit that information to another controller(Xcoobee.com,2018).

6. *Privacy by design*

The data controller shall implement suitable specialized and hierarchical measures in a viable way with a specific end goal to meet the necessities of this Regulation and secure the privileges of data subjects. Moreover, Article 23 calls for controllers to hold and process only the information necessary for the completion of its data minimization and constraining the access to individual information to those expecting to showcase the processing (Xcoobee.com,2018).

7. *Potential data protection officers*

All the organizations need to appoint a Data protection officer (DPO) according to the GDPR legislation. Associations should give the contact details of their officer to their data protection authority. The activity of the data protection officer is to illuminate and guide the association about gathering GDPR necessities and observing compliance. They'll likewise go about as the data protection specialist's essential purpose of contact and will be relied upon to coordinate with the expert. The DPO elected must be proficient in data protection law and practices. They must be provided with all the resources to carry on their duties and they should report specifically to the highest level of administration(Burgess,2018).

The organizations can be fined for not having appointed officers. In case of security breach, it can also be fined. The money related penalties will be settled on by Denham's office and the small offenses could bring about fines of up to €10 million or two percent of an association's worldwide turnover and those with high results can have fines of up to €20 million or four percent of a company's worldwide turnover which is very huge. (Burgess,2018)

1.4. GDPR will affect

GDPR will affect the two groups - data controllers and data processors.

Data controllers are the ones who state why and how are the individual data processed. They can be any government or private organization. Processors are the ones who do the actual processing of data like an IT firm doing the information handling. Regardless of whether controllers and processors are based outside the EU, the GDPR will even now apply to them so far as they're managing data belonging to EU inhabitant. Data controllers have some obligations to ensure that the data is processed properly. They are supposed to fairly obtain and process data and keep it for one or more specified and lawful purpose. Personal data should be used only in ways which are compatible with the purposes for which it was given to the data controller. Personal data should be kept safe and secure, accurate and updated (Curtis, 2018).

As per GDPR the controllers and processors must be direct about how they assemble data, what they do with it, and how they process it and must be clear in disclosing these things to people. Everyone has the right to get to any information an organization holds tight on them, and the benefit to know why that data is being taken care of, to what degree it's secured for, and who gets the chance to see it. Where possible, data controllers should give secure, manage access for people to review what information a controller stores about them. On the off chance that the information is mixed up or divided, people can ask for it to be amended at whatever point they require (Curtis, 2018).

There's a need documentation of why individuals' data is being gathered and prepared, description of the data that is held, to what extent it's being kept for and depictions of specialized safety efforts set up if the organization have more than 250 employees(Burgess,2018).

1.6. GDPR and BREXIT

Indeed, the UK is leaving the EU but since the UK government just activated Article 50 in March 2017, which gets under way the demonstration of leaving the EU inside a two-year time span (however it could take longer), this implies GDPR will produce results before the legitimate outcomes of the Brexit vote, which means the UK should in any case go along. Also, the implementation of the new data protection bill by UK will include almost all the provisions of the GDPR. The Data Protection Bill is right now going through debates in the House of Commons and House of Lords. It is liable to various potential alterations, which all must be affirmed by the two houses previously the Bill can be passed and turned into an Act of parliament (*Curtis,2018)***.**

2. Impact of GDPR

GDPR will achieve another level of straightforwardness into data gathering, stockpiling and use. It will create the requirement for more compliance spending. It will ensure if the organization's operational procedures are up to the most recent standards or not and the current innovation is composed and upgraded to the most recent protocols. In addition, a few organizations and associations should procure a compliance officer to help screen and deal with any data accumulation battles. (*Coredna,2018*)

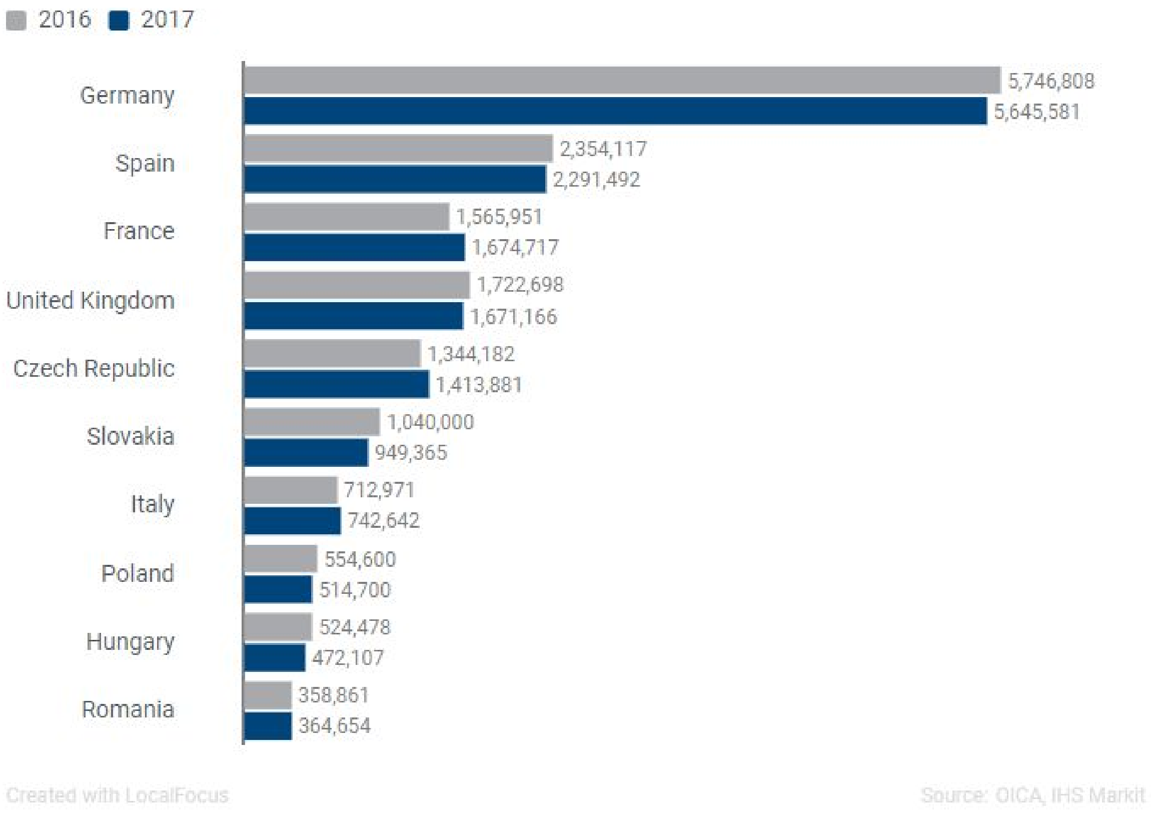
Notwithstanding, these expenses will motivate trust and confidence between the organization and the clients and so it shouldn't be viewed as an extra cost. Organizations that manhandle personal data of individuals will be seen less reliable according to general society especially if they're hit with the net revenue busting fines. On the other side, the organizations that esteem access and utilization of their client's information and regard it as a benefit, rather than a right, will set themselves as dependable and trustworthy organizations in the coming years(*Coredna,2018*)**.**

2.1. GDPR and European Automobile Industry

The European Automobile Manufacturers Association (ACEA) acts as an advocate for European automobile industry by representing all manufacturers of automobiles which produces cars, trucks, buses, and vans at various sites in Europe. The European Automobile Manufacturers' Association (ACEA) consists of 15 Europe-based automobile companies as its members like Volkswagen, Honda, Toyota, Fiat, Volvo, BMW group and other major companies (ACEA, 2018).

2.1.1. Production

Looking into key figures for production of motor vehicles in 2016, around 96.1 million units were produced in the world. Out of which around 19.2 million units were produced in Europe consisting of 28 countries before Brexit. But passenger cars specifically hold around 77.7 million units in the world out of which 21% (16.5 million units) were produced in Europe (ACEA, 2016).



Source: OICA, IHS Markit

2.1.2. Vehicles in Use

Considering vehicles in use, around 256.1 million units of motor vehicles were in use in Europe. The passenger cars in Europe hold around 256.1 million units with 573 units per 1000 inhabitants with an average age of vehicle to be 10.7 years (ACEA, 2017).

2.1.3. Revenue generation

The total revenue generation by few automobiles companies having a worldwide presence can be shown in the following table. The companies will have to face severe fines if they don’t follow the General Data Protection Regulations after being compliant with in. If the

GDPR is broken by any organization then the company must pay a fine of 4% of annual global revenue generated by the company (Statista, 2016).

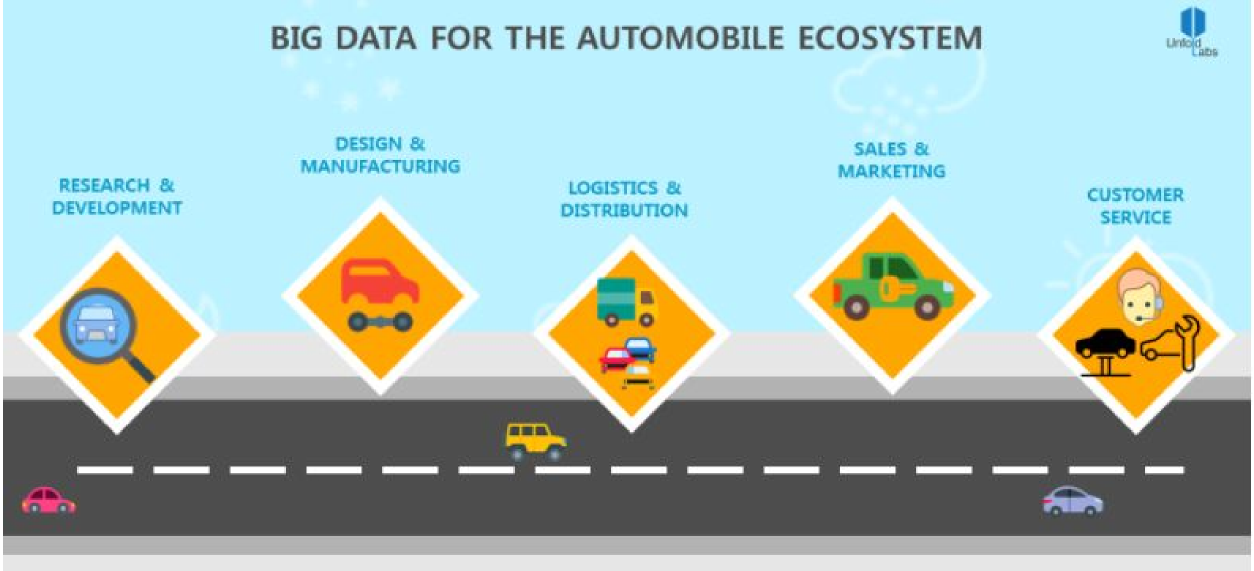
	AUTOMOBILE COMPANY	**OVERALL REVENUE FY 2016 (in billion U.S dollars)**	**Fine (4% of Revenue of the company in that FY)**
1.	BMW Group	104.13	4.1652
2.	HONDA	129.2	5.168
3.	VOLKSWAGEN	240.26	9.6104
4.	TOYOTA	254.69	10.1876
5.	FIAT (FCA)	116.96	4.6784
6.	FORD	151.8	6.072
7.	DAIMLER	169.48	6.7792

Calculating the overall revenue for below mention companies gives us a fair idea about the fine system which companies will have to face for being non-compliant to GDPR.

2.1.4. Type of data collected and data collection technologies

Focusing on the number of passenger connected-cars and other motor vehicles like trucks, vans, buses in use in Europe, it is evident that the data collected from connected-cars and other motor vehicles are at maxima and needs to be collected and processed precisely. The data collected from the connected passenger vehicles are used mainly for Research & Development, Design & Manufacturing, Logistics & Distribution, Sales & Marketing and Customer Service (BMASS, 2017).

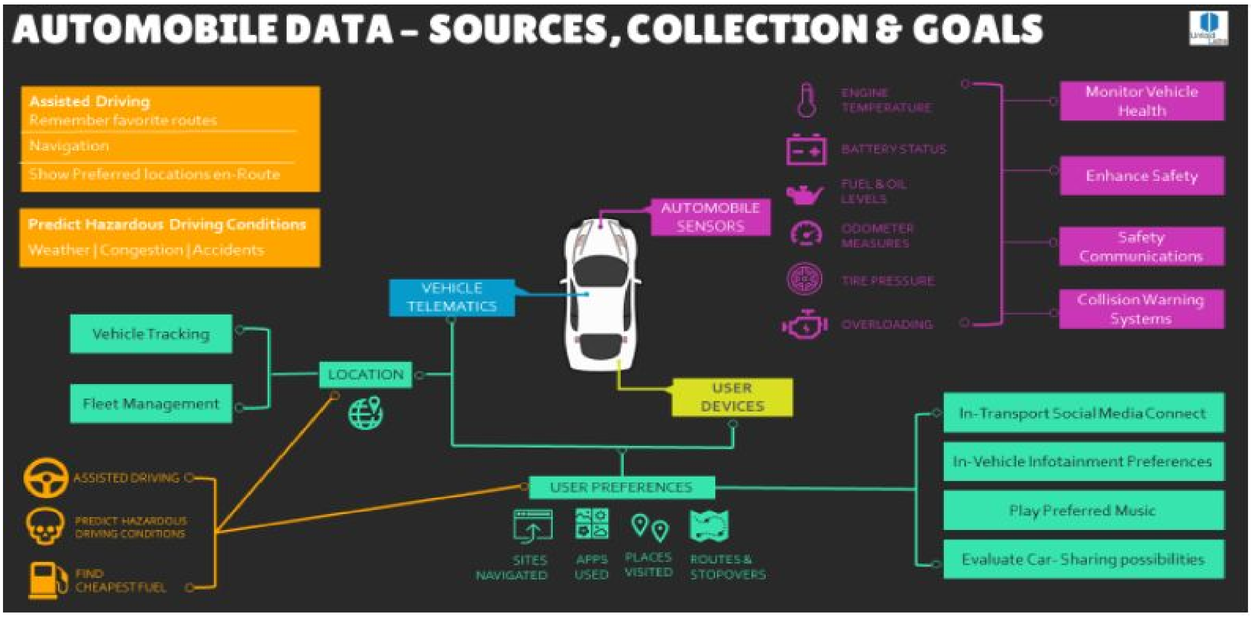
While and after buying any automobile, companies collect general data from the users and further analyze the data and make a predictive analysis to meet the future demands from consumers. But companies do track other activities which consumer do while they are using cars.



Source: Business Mobility as a Service (BMASS).

It starts with tracking phone calls, texts, accessed websites, radio stations tuned, speed limit monitoring etc. Some national governments have installed black boxes in cars which record and collect data like speed and seatbelt positions before and after a crash. Most of the car companies know the travelling pattern of their customers with in-dash navigation systems. For example, every time a customer heads to service their cars, companies do make a note of distance travelled by car and accordingly make a predict the demand for spares, that might come from the consumer. Use of such technologies helps the firm to deliver customer satisfaction and on-time performance (Quain, 2017).

Looking at data collection techniques in automobile industry, the data collected from various vehicles are based on sensors embedded in various devices installed in cars to track, record and monitor the performance. The new technologies were introduced recently which are still used in almost all the vehicles. To get the information about the location of the vehicle and routes passenger has taken in their journey can be collected by in-built navigation system of car. Whereas cameras and sensors are used to know the surrounding of the car to get immediate information about weather conditions, traffics and more. The automobile company collects these data and revert back information like lane-changing warning, brake assistance and parking detection. Nowadays, in-cabin information is easily collected through microphones, cameras and other devices which connects passenger with emergency services at times of failure or crash. The modified cars use facial recognition or biometrics to get information about the user to allow access to the car by recognizing the passenger by adjusting into system. When it comes to integration of commonly used mobile devices these days with the cars by simply connecting them with the help of apps provided by android or ios like car-play, android auto and other applications. These apps when used might expose data from these cars to the application providers as we already accept their privacy policies in order to use the applications (NADA, 2017).



Source: Business Mobility as a Service (BMASS).

2.2. Challenges faced by Automobile Sector by becoming GDPR compliant

Data collection process of firms providing goods and services to consumers will be affected and must be changed in accordance with governing policies. According to factual explanations, 96% of businesses are unprepared and have very less knowledge about GDPR compliance. This knowledge gap will create several challenges to automobile industry. All original equipment manufacturers (OEMs) must take this issue seriously by ensuring that they comply with GDPR and follow data protection requirements connected to all automobiles currently and in future as well. All cars which make use of equipment involved in data collection must be either removed or regulations should be implemented to avoid data breach (BearingPoint Institute, c2017).

2.2.1. Data Storage and Breach

The amount of data, whether it is personal or non-personal must be securely collected and processed across the organisation. Due to GDPR, organisations will have to ensure that the data stored on multiple platforms globally or locally is only accessed by assigned person for the use of business only. The organisation should be able to track the data sources and audit them to have a fair idea about who, where and when is accessing the data (Consultancy.uk, 2017).

In a situation of data breach, the organisation must send a notification to respective individual specifying the potential data breach, before 72 hours. Organisation will have to pass this notification to higher authority within the firm, who is responsible for data breach issue (GDPR Articles 33 and 34).

Thus, the challenge here will be to appoint Data Processing Officer who will look after the sources and end users of data within and outside of the organisation. The organisation will have to change or update their existing technology and organizational practices with regards to data collecting and processing (Good, 2018).

2.2.2. Consent

The organisation will have to take a prior consent about collecting personal data before proceeding with providing any services or goods as per the requirement of GDPR articles mentioned in the amendment. The organisation will have to assure that proper consent was taken and has acquired agreement from an individual for the use of their personal data for the company's operations. Thus, asking for consent every time will lengthen the procedures and would give rise to delay in processing of further tasks (BearingPoint Institute, c2017).

2.2.3. Cross-Functional Team Aligning

The organisation will have to align all the teams to approach GDPR consistently. The alignment of each team across the organisation which includes sales, marketing, customer service, IT, accounts and others, is very crucial. While working in the organisation, every employee should be given prior training and awareness needs to be created about GDPR compliant. When working with various forms of data, all the employees should be supervised by team leads of each department to ensure that data is not being compromised and if it does happen then issues are raised to higher authorities and further actions would be taken against that employee or team whoever is involved in the process. Therefore, to align all the teams to make them work parallel on the same platform flexibly without violating the rules and regulation under GDPR compliance act is a major challenge for any company to apply across the organisation within a very less time frame *(Hegde, 2017).*

2.2.4. Privacy by Design and Default

Under GDPR compliance the organisation must ensure that the privacy and data of an individual is protected throughout. Article number 25, about the privacy by design and default has raised a challenge for the organisation to redesign the privacy terms and conditions for the end users and setting it as default. The data protection by design involves segregating and integrating data in an organized form to eliminate the data processing time. Whereas, data protection by default involves that the data collected by any organisation needs to be processed and stored only until it is necessary. Hence, putting limitations to minimize data collection for specific purpose. Also, providing default service of end-to-end security for a specified period to the consumers is necessary without enforcing them to agree on mentioned company's terms and conditions. Therefore, to design a structure or an architecture of privacy settings by default to let users have their privacy and data secured would be a major task for automobile industry to limit the data access (Davis, 2017).

3. Infrastructure Requirements

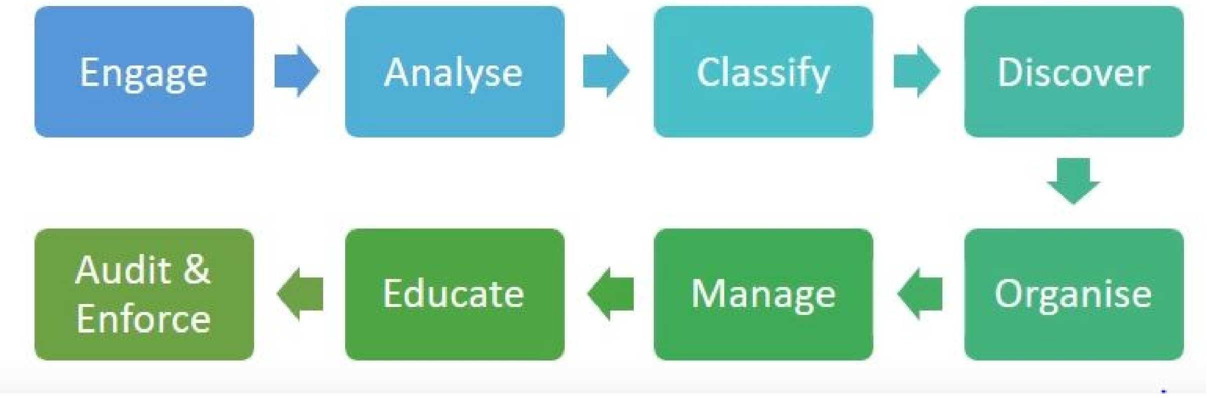


Fig.3.1. GDPR - ideas for analysing your data. Source: https://www.youtube.com/watch?v=eJBXUajwK_U&t=1251s

General Data Protection Regulation is set to be in action from 25th May 2018. With extensive requirements to comply with this policy, organizations need to invest in technology and intelligent analytical systems. Many software firms exist in the market, which provide solutions to tackle this issue. Depending on the scale of organizations, a choice could be made on availability and product efficiency. All software products that implement solutions for compliance, follow a basic flow of information. It is mandatory to keep an eye on each of the sub functions to eliminate possible conflicts with data management. Sub functions required to be GDPR compliant are shown in the flowchart (*Figure 3.1*). Infrastructure requirements are listed below.

3.1. *Data Classification and Storage requirements*

Data comes either in structured or unstructured format. These can be generated by humans or by machines. A common example of structured data: Date of Birth, Phone numbers, SSN/PPSN, Insurance numbers, Passport numbers etc. These strings have RDBMS structure and can be easily searched by use of simple SQL queries. On the other hand, unstructured data is all that doesn't fit in the description for structured data and can also be stored in a non-relational database. Unstructured data may be images, videos, email, text messages, sensor data, surveillance data etc (*Datamation, 2018)*. Considering the automobile industry, all the new cars that are launched have state of the art infotainment systems and sensors that make cars more autonomous. Millions of information is collected via these sensors and systems. Once data is classified in either forms, further processing can be done, and information can be handled accordingly.

With enormous amount of data flow, it is important for organizations to manage storage and security of data.. It is suggested that operation of cloud storage is relatively inexpensive when compared to onsite servers (*Hall, 2017*). All discovery algorithms can be efficiently applied to cloud databases, enabling seamless management of information. Regulations can be implemented and access rights, will provide security forefront to safeguard data.

Cloud solutions could be implemented from any of the tech giants in the market, a few examples: Amazon Web Services, EnterpriseDB, Google Cloud SQL, RackSpace etc. It is important to choose the type of storage cluster, as it might affect performance. Personal cloud cluster available for storage can be easily used with EU specific requirements and their ability to be easily integrated with other network services and components makes it reliable. These systems can be scaled as per requirements (*OnLineTech, 2018*).

3.2. Data Centers

With millions of new age vehicles on the road, it is expected to have data collection in a range of Zettabytes. To sustain incidents like massive theft of data, hardware failures, natural calamities etc, it is important that the automobile industry has data centers established in a probable risk-free zone across the EU. Data centers provide comprehensive backup of data and ensures safety of stored information (*Chopra, 2012*), all with requirement of less human supervision.

3.3. Data Integrity requirements

With all arriving data being carefully sorted and stored appropriately, it is now important for systems to run an integrity check to reconcile with accuracy of data being received. Pattern mapping algorithms can be used post integrity checks, to identify potential NPPI data. All NPPI data must be suitably encrypted before storage or should be subjected to instant purging.

Integrity checks are essential part of the process to ensure that data is valid. Software programmers could define various constraints by use of primary keys and foreign keys. To maintain a relational structure of the database, referential integrity constraints could be deployed (*Sybase Inc., 2009*). In business terminology, referential integrity defines a set of business rules that apply to all incoming data (*Hendrix, 2017*). Violation of RI could lead to population of junk or dropped values. For a data to be useful for business, it is essential for all the information to be correct including the rules, relation compliance etc. Algorithms could be defined in databases to ensure data integrity (*Teeling, 2012*).

The process of integrity check enables the businesses to make sure that the data has remained untouched from either end points. In terms of security perspective, a data integrity service provides auditable trail for reliability of information. Often such data gets corrupted accidentally or gets modified by unauthorized person. It is now highly important for data security experts to devise practices that provide reliable and unaltered data.

3.4. Data Security and Reporting requirements

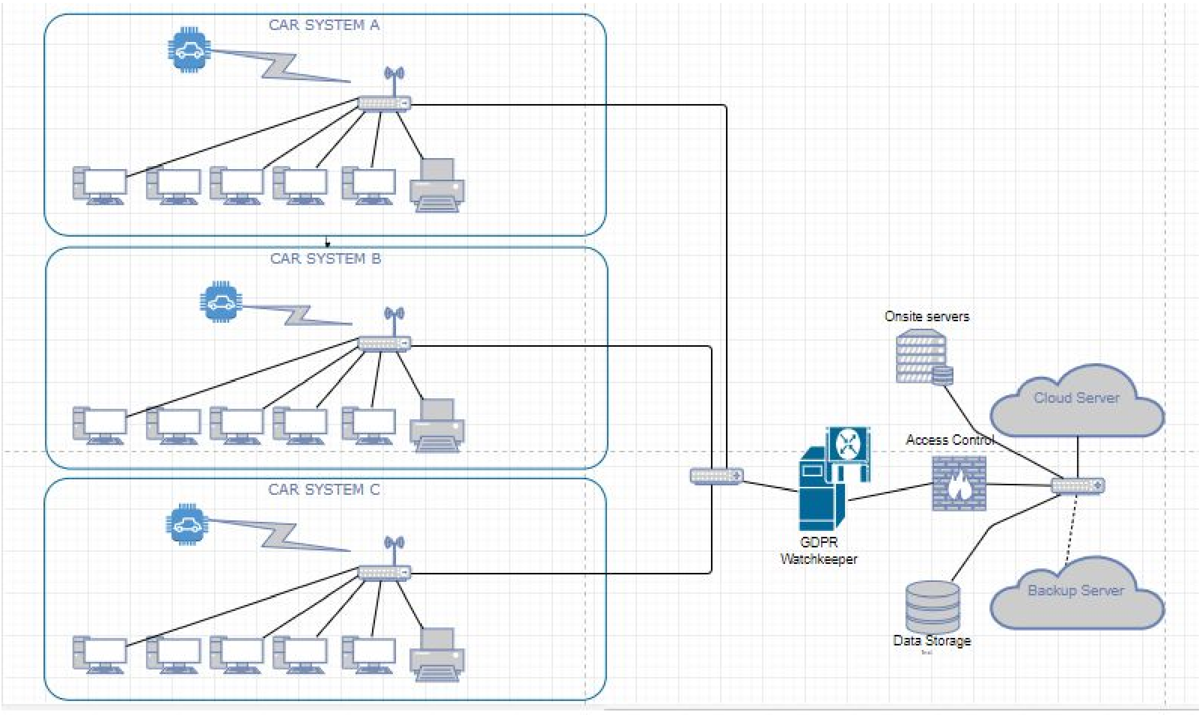


Fig 3.4: Proposed data flow for vehicles. Source: Varghese, S.S. 2018, tool used: www.draw.io

Terminal requirements apart from storage, is the need of web servers for management of tiny bits of information. All network communication and system ping routed through server is recorded. Use of standard web servers, e.g. Apache, NGINX, etc provide reliable options for data communication through websites. When configured to GDPR standards, only allowable data could be transmitted and monitored with generation of log messages.

As discussed under the Data Visibility section, it is mandatory for all bits of similar information across various systems to be visible without any ambiguity. Enabling automated reporting services makes sure that the business can keep track of storage of compliant data, without human intervention.

The above diagram is a pictorial representation of the information collection network for vehicular systems. Various sensors act in complete autonomy and send data received through its systems, to the mainframe or backend server. These data may have personal information about the driver, his connected phone, IP addresses, Map routes, etc. All these transmitted data which will be further analysed by the firm, must pass through enforced compliant systems to ensure that only required information is gathered with the consent of the individual. It will be mandatory to enforce standards as per GDPR act, onto various systems, to ensure safety of information. In further sections, ways to ensure compliance to GDPR act will be discussed.

3.5. Artificial Intelligence

Deployment of AI system in accordance with other subsystems would lead to efficient monitoring of data pipelines. Pattern mapping algorithms could be imbibed into AI module to track changes. All connected clients could be simultaneously monitored and SQL statements to retrieve saved data, can be deeply analysed. AI system will also provide autonomous handling of NPPI data, making the system more efficient. Automated decision making for data will prove crucial to comply with regulatory standards (EDPS, 2016). Proper configuration and assessed feedback loops to machine learning system will enable the AI system to follow non-biased standards when handling sensitive information.

4. Business Challenges

Aspects that are made mandatory after the enforcements of GDPR are Data Integrity, Data visibility, data Monitoring, Data Security, Data Recovery and Log Management:

4.1. Data Visibility

When the auditors will be coming to check the compliance of GDPR, the first they will check At the point when the Auditors will come to check the consistency for GDPR, the primary thing that they will check is the company's awareness about the presence of their client's information in different interfaces and their respective infrastructure. Also, the measures were taken by the company in terms of data protection and security. The companies will have to demonstrate that they have access to tools that provide visibility to its users and how they access and use data and enable the company to run regular compliance assessment reports (*Thin air, 2017*).

The companies can reduce the risks of non-compliance and decrease the internal cost of investigating and reporting a breach if they design the tools that can provide the information that is needed to quickly understand how the customer data was accessed and used, during the investigation. This requires will required companies to achieve real-time visibility over the data. (*Thin air, 2017*). The articles 7, 8 and 35 covers the regulations made by GDPR concerning Data visibility (*Ping Identity, 2018*).

4.2. Data Integrity

Data integrity ensures that the data characteristics like business rules, relations, dates and definitions are complete. Whenever a database is designed and is authenticated through the current use of error checking and validation routines, data integrity needs to be imposed. The entire data integrity process ensures that the data has remained unchanged right from the data creation and data reception. Data integrity ensures that the information is the similar as it was inputted and is auditable to confirm its reliability (*Vera Code, 2012*).

With the explosion of new technologies, saving the unstructured data files such as images, audio files etc, the threat of data corruption has increased (*BMC, 2018*). Under the Article 32 GDPR has made it mandatory for the companies to have a data integrity process in place. The article 32 relates to the following aspects of the data: data completeness, data accuracy, consistency and maintenance (*Article. 32 GDPR*)

4.3. Data Security

As per the GDPR, the new security requirements consider the data protection authorities' previous experience and the new digital environment, in which cyber-criminals trade personal data of the users to the underground data markets. The technical measured that needs to be ensured under the GDPR are:

Properly configured firewalls updated with the latest software's. User access control management, which ensures that there should be no one person in the company with the access to all files and ensure restricted access. Regular software updates, using patch management softwares and data backup *(Lexology.com , 2018*).

4.4. Disaster Recovery

It's imperative for the organisation to have a reliable disaster recovery plan in place to ensure that the business is properly prepared to deal with any disaster that might strike, to get back up and running causing minimum business impact.as soon as possible *(CSO, 2018)*.

4.5. Log Management

Any web application stores and records the user activity in server logs that contains information classified as personal data by default under the European Union's General Data

Protection Regulation. As per the GDPR this personal information includes, the IP addresses that are specifically defined as personal data per Article 4. In some cases, the logs also contain usernames if company uses them as part of their URL structure (*Ctrl blog, 2018*). Hence, as per the new requirement in GDPR it is required for the companies to make implement log management tools, that can monitor all user and system activities to identify suspicious behaviour.

5. Solution to the Business Challenge

Source: www.dbnetworks.com

The DB Networks introduced an artificial intelligence-based product, DBN-6300 to support companies and their GDPR advisors in preparation of the new EU regulation. It offers an artificial intelligence-based database security for data visibility, data security from internal and external threats, and detailed SQL analysis. By delivering the insights and situational awareness of company's database infrastructure, it ensures that the companies can have a real-time assessment to immediately identify attacks and its employees compromised credentials *(Dbnetworks.com, 2018)*.

The DBN-6300 is easy to set up and can be deployed with any alterations to the existing applications, databases, or cybersecurity systems. It highlights on the company's entire database infrastructure, reduces the time and effort taken to document every structured data stored. And after discovering all the required personal data, it produces the exact personal data inventory *(Dbnetworks.com, 2018)*.

The DBN 6300 combines network monitoring, performs detailed analysis of every database activity on the network, and an adaptive model to create and maintain a corporate policy to segregate between the safe and unauthorised transaction. DBN-6300 discovers the databases that are undocumented and/or non-compliant. It provides the insights on data in motion, including the interaction of application to their respective databases, using highly accurate machine learning algorithm that stops database attacks in real time *(Dbnetworks.com, 2018)*.

The DBN-6300, assists companies in complying with the GDPR regardless of the flow, storage or processing of the data, GDPR has made it mandatory for the organisations to respect and protect the personal data. Hence, companies whose employees, customers and goods for sale are in the EU have started identifying and mapping the processing of all the personal data of the user *(Dbnetworks.com, 2018)*.

The Artificial intelligence based DBN-6300 works on a non-obstructive network where it creates a copy of the database traffic. An analysis is applied to discover all database instances, map the databases to their connected applications, and collect database User Behaviour Analytics (UBA). Then, statistical and machine learning analysis are applied to discover the database threats that were previously not visible, to the security team. As a result, security team will have visibility and improved operational intelligence from their database system, and will be notified when important database infrastructure events occur (*Dbnetworks.com, 2018)*.

The DBN-6300 can trace any unidentified databases that may contain personal data, plot the flow of the traffic to automatically document where the personal data is being processed, identify database attacks, and use of any compromised credentials (*Dbnetworks.com, 2018)*.

5.1. Phases in DB network Framework

5.1.1. Baselining the Database Infrastructure

Under this phase, a machine learning algorithm model of normal behaviour is created. The portion of the network and database activity that deviates from the normal model is then identified. This model is then trained based on the inferences studied based on the normal behaviour of the database activities to draw the exact picture of stable database activities. The definition of normal database activities is made after considering the characteristics like the clients and servers IP address, port, and the database user account that is being accessed. The DBN-6300 then builds a map of all the data activities observed across the network. It automatically creates a behavioural model based on those database activities that are normal. This benchmark for normal behaviour is then reached when respective database activity is consistent over time (*Dbnetworks.com, 2018)*.

5.1.2. Stability Analysis

Based on the stable model obtained from the previous phase, the data base activities that deviate from the normal behaviour of database activities are identified as threat (*Dbnetworks.com, 2018)*.

5.1.3. Ongoing Monitoring

With a benchmark of normal data base behaviour obtained in the first phase, and definition of active threat, during the ongoing monitoring, the behavioural changes that are mapped as threats to the database environment are continuously monitored. Such changes are associated with a new risk that needs to be managed; DBN-6300 offers a risk factor to focus the attention on the most significant anomalies. Lastly, DBN-6300 offers a data analysis and visualisation through the dashboards (*Figure 5.1.3*). This dashboards layer offers a detailed process of all the data flows in the system and focus the attention to critical areas, quickly and efficiently. It also provides the facility to generate manual monitoring rules based on the user preferences.

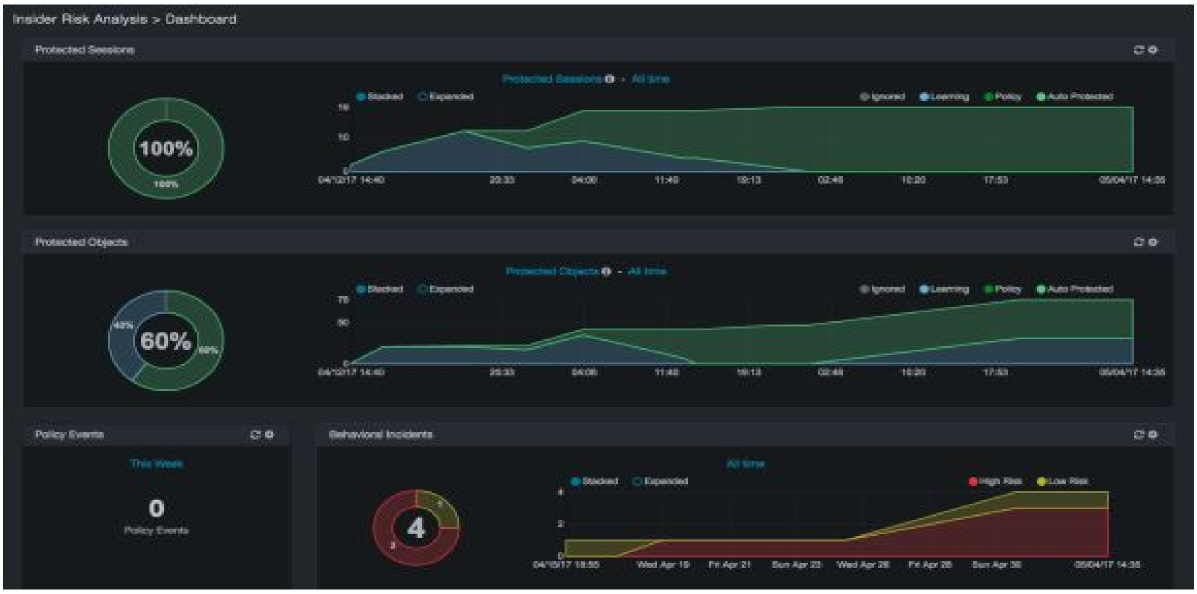
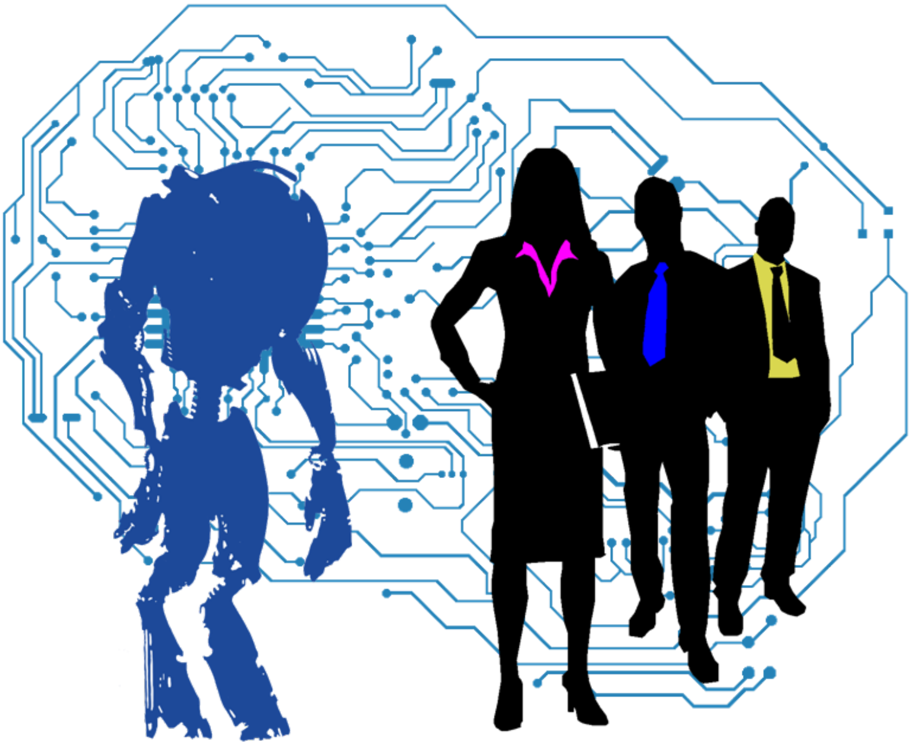


Figure 5.1.3 Source: www.dbnetworks.com

6. What will we achieve?



6.1. Use AI to create a red flag system

Using the artificial intelligence, the companies will be able to priorities the valuable time of their legal staff. AI has got the ability to look can into tens of thousands of legal contracts in one afternoon, a task that would take lawyers weeks. Artificial intelligence will automate the critical aspects of the GDPR by applying algorithms to identify the places where personal data is stored even in the places that lawyers would never find (*Globallegalpost.com 2018*).

6.2. Predict your data controller and data processor scenarios

GDPR has made it mandatory for the service provider and other third-party vendors in the automobile industry to categories themselves into data controllers and data processors to understand their responsibility. However, deciding whether the vendor is a data controller or data processor, is quite difficult and is topic of debate. Using the correct data, AI will automatically categorise these relationships and categories the service providers into the two categories (*Globallegalpost.com 2018*).

6.3. Keep it simple

Due to complex business operations, the companies are more exposed to the failure of complying with the GDPR. In such scenarios, it is of utmost importance for the key employees to have the clear awareness about the data protection acts and understand the impact on business due to non-compliance. In this case, AI will help by assisting the identification of systems and activities where sceptic data protection problems are likely to occur by enabling the companies to take more intensive compliance steps in some areas whilst keeping other areas simplified (*Globallegalpost.com 2018*).

6.4. Minimise and anonymise

The simplest way to ensure 100 percent compliance with GDPR is not to process any personal data. That’s impractical for most businesses, but it is also true that the less personally identifiable data the organisation holds, the lower the risk. Until recently, anonymization technology was regarded as quite niche. Now that GDPR carries specific requirements for anonymization, the technology is no longer a nice to have – businesses should be considering it as a matter of priority. Artificial intelligence technology can help automate redaction, in order to comply with GDPR requirements. A tight grip on the data life-cycle process will also help businesses minimise the amount of personal data they hold. Again, AI technology can help identify and delete personal data that it is not necessary for the business to store. Generally, companies hold more personal data than they need. Often it is more important to understand the attributes of a person, rather than their individual identity – what you are, not who you are (*Globallegalpost.com 2018*).

6.5. Legal advisors

Legal advisors – internal and external – have a key role in suggesting practical measures to address GDPR risks. Time spent automating legal assessment of data protection liabilities will pay dividends given the now-increased risk-cost of GDPR. For some businesses, this will generate competitive advantage because the organisation will be more able to leverage the power of data without introducing the heavy restrictions that would be required without access to automation tools (*Globallegalpost.com 2018*).

6.6. AI helps compliance

GDPR is set to impose harsh penalties for non-compliance, yet achieving the correct application of some of its principles will be subjective. AI can help manage the additional investment in data protection resources required to address GDPR and help experts tasked with data protection compliance keep on top of the thousands and even millions of decisions that need to be made about personally identifiable data every day. For some businesses AI-driven automation will be critical to achieving any level of real world compliance (*Globallegalpost.com 2018*).

7. Recommendations

Since GDPR is on the door and is very strict related to the use of customers privacy data which companies uses as part of the product development and marketing strategies, all companies are required to act quickly to save them from the big fines and penalties which they would be charged with in case of policy breach process. It is essential for the organisation to plan their approach for GDPR compliance. There are recommendations for the companies which they should place their focus on to fully comply with GDPR regulations.

7.1. Documentation of the current information stored

Every company should document the information which they had stored and are currently collecting from their customers as part of data collection process. It is important for each company in the industry sector to know all the data they have collected and are collecting from their existing customers as GDPR is directly involved with the data protection and rights of customer privacy. Since, in present companies are collecting all type of data of customers for making new strategies to market and develop new products. All industries are required to document these data type which will make it easy to audit and understand which data they must keep and to be removed from the database to meet the GDPR regulations.

7.2. Restructure and Communication of privacy information

These days customers are more concerned about their privacy data which companies are capturing as part of their data collection process. Currently, for every product purchase there comes a privacy terms and condition list which states that company will collect the data of device functioning for development of the products but does not states which type of data they are going to collect as part of the process. Companies are required to restructure their privacy policy in which they must explain in legitimate manner which type of data they would need for the further product development and research in their privacy documentation in accordance with the GDPR regulations. They also need to communicate all these information to their customers to make them aware of the type of data which they are going to share with the companies under privacy policies.

7.3. Create and plan procedure and timelines to handle new requests

Companies are required to review their current procedures and GDPR regulations. They need to plan new procedures to handle the requests and create a timeline to apply these new procedures step by step within the provided timescales and should also look for the other additional information which needs to be provided as part of GDPR compliance. This is important to make sure all procedures are being followed and are within the timescales provided to comply with new regulations and to make sure all the requests are fulfilled to avoid the unnecessary complications.

7.4. Documentation of Laws for processing personal data

GDPR comes with different sets of law to regulate the personal data collected and used by the companies by processing activities of customers. There are many articles which describe the new regulations and limits the data processing for the companies. Companies should document all these laws and articles while upgrading their procedures of data processing and should create plans considering these laws and should update their privacy policies to comply with the regulations. They should use highly legitimate way while documenting all the policy to ensure that no law is broken in the process and are complied with the GDPR regulations.

7.5. Individual rights

There many new articles are incorporated under the GDPR which can be accessed by the individuals under the current regime. Some important rights which every organisation should concern about are *"Article 17 – The right to erasure, Article 18 – The right to restriction of processing and Article 20 – The right to data portability"* (Inman, I., 2017). All these rights limits organisation from processing personal data of individuals without their knowledge, these rights also restrict them from sharing these personal data with another organisation directly or indirectly. The companies should create the procedures specifically to ensure that all these rights have been met which includes the deleting the personal data which needs to be according to the regulations.

7.6. Data Consent

Under data protection law, Data consent is an important factor which contains several criteria to be met for a consent to be valid. These consents must be freely given a choice to individuals, should be very specific in nature, completely informed, free from unambiguous actions and should be positively indicated. Companies should review all the consents they want to seek, record and manage as part of data processing. Should list the changes needed to be done in the database. They should also focus on the previous database and should refresh the existing consents at this stage if they are not meeting the GDPR regulated standards.

7.7. Data breaches

Data breach under protection law will result in heavy penalties for the companies which may go in billions of euros. To avoid these situations companies had to create new procedures in place which will lead them in detecting, reporting and investigation of any personal data breach. They can use different tools suggested in the report as these tools are designed specifically to process the data which comply with the GDPR regulations, these tools can detect and report any type of data breach and make sure no regulation has been passed in the process of monitoring personal data by the companies. The tool will be operated by data protection team to monitor all the data processed within the organisation.

7.8. Data Protection Team

Companies should now consider of creating a data regulatory body within the organisation structure to govern the complete process of new regulations. This team should have a data protection officer and would be responsible for all the data processing and will ensure the data protection regulations are being followed at each step. The team will receive a report from the GDPR compliance tools which will give the details of data processed within the organisations and will report any data breach which will enable them to take necessary actions. Since, the tool is an automated software it requires low team size to monitor the process. This is important as companies should ensure all the procedures of new data protection regulations are in place to avoid any chance of passing the laws. They should consider this weather they need a new team or can upgrade any existing team for this task.

7.9. International Operations

Since most of the automobile companies are working across borders in different countries it is more likely for data to be shared across borders. The GDPR articles 44,45 restricts companies from sharing the data across borders and it can only be done after providing adequate reasons and protection of personal data. To prepare for this companies should review their business operations plans and identify all the circumstances under which they can transfer personal data across borders and ensure the end to end data protections by placing a transfer mechanism which complies with the GDPR requirements. The article 46 allows organisations to share the privacy data with public authorities of the country. For this organisation does not require any authorization from data protection commissioner, they only must maintain the GDPR requirements (Gabel, D.D. & Hickman, T., 2017).

7.10. Future development consideration

Organisations are now into developing more technology based automotive like autonomous vehicles which is based on AI technology. Since, AI technology is completely based on the software programming and to develop this companies need to collect different type of data to analyse and store for the development. This means that organisations are required to build corporate investment plan and build strategies which can be used for better access of consolidated and cleaner data that are incorporated with new GDPR rules which are strictly against the misuse of personal data of EU citizens.

8. Conclusion

Automobile industry is one of the biggest sector and is rapidly growing with new technology development like smart cars and autonomous cars which requires lots of different type of data and analysis. New GDPR rules limits the organisations to access customers personal data which makes it difficult for them to conduct and proceed with the research and development of new technology.

In this report we have outlined the effects of GDPR on automobile sector research and development in terms of personal data collection and usage of EU citizens. Considering the new regulations all organisations are expected to restructure their current process of data collection and processing structure to avoid the threat of heavy penalties which will be imposed in case of overpassing these laws. As these regulation are also applicable on the data which all organisations are holding at present, it is important to analyze all of current and update according to the regulations which also means that companies have to delete some of the data from their database.

9. References

ACEA, 2017. *EU Production.* [Online]
Available at: http://www.acea.be/statistics/tag/category/eu-production [Accessed 10 April 2018].

ACEA, 2017. *Vehicles Per Capita, by country.* [Online] Available at: http://www.acea.be/statistics/article/vehicles-per-capita-by-country [Accessed 10 April 2018].

ACEA, 2018. *ACEA Members.* [Online] Available at: http://www.acea.be/about-acea/acea-members [Accessed 10 April 2018].

Anon, 2017. Car dealers urged to act now on 12-steps to GDPR compliance. *AM Online*. Available at: https://www.am-online.com/news/market-insight/2017/08/11/car-dealers-urged-to-act-now-on-12-steps-to-gdpr-compliance [Accessed April 9, 2018].

Anon, 2017. How GDPR regulation changes will impact your fleet. *Corporate Vehicle Rental in Shropshire*. Available at: https://www.fvsl.co.uk/blog/gdpr-regulation-changes-fleet-industry/ [Accessed April 7, 2018].

Conroy B., 2017. What Should the Auto Industry Do About New European Data Rules? *IoT Evolution World*. Available at: http://www.iotevolutionworld.com/smart-transport/articles/434511-what-should-auto-industry-about-new-european-data.htm [Accessed April 8, 2018].

Anon, 2017. Should we regulate artificial intelligence? *JD Supra*. Available at: https://www.jdsupra.com/legalnews/should-we-regulate-artificial-76349/ [Accessed April 13, 2018].

Art. 32 GDPR – Security of processing | General Data Protection Regulation (GDPR). [online] Available at: https://gdpr-info.eu/art-32-gdpr/ [Accessed 9 Apr. 2018].

Baxter, B. (2018). How to make your disaster recovery GDPR compliant. [online] CSO Online. Available at: https://www.csoonline.com/article/3212250/compliance/gdpr-how-to-make-your-dr-compliant.html [Accessed 10 Apr. 2018].

BearingPoint Institute, c2017. *Connected cars and privacy: shifting gear for GDPR?.* [Online] Available at: https://www.bearingpoint.com/files/BEI008_06_GDPR_Connected-cars-and-privacy-shifting-gear-for-GDPR_final.pdf&download=0&itemId=434626 [Accessed 19 March 2018].

BMASS, 2017. *One for the road — big data & the automobile industry.* [Online] Available at: https://www.businessmaas.com/connected-car/self-driving/one-road%E2%80%8A-%E2%80%8Abig-data-automobile-industry/ [Accessed 11 April 2018].

Chopra, P., 2012. *WHY BUSINESSES NEED DATA CENTER SERVICES?.* [Online] Available at: http://www.datacenterjournal.com/why-businesses-need-data-center-services/ [Accessed 19 March 2018].

CMOD, 2008. *Protecting the confidentiality of Personal Data.* [Online] Available at: https://www.dataprotection.ie/documents/guidance/GuidanceFinance.pdf [Accessed 26 March 2018].

Consultancy.uk, 2017. *Five critical challenges related to becoming GDPR compliant.* [Online] Available at: https://www.consultancy.uk/news/13474/five-critical-challenges-related-to-becoming-gdpr-compliant [Accessed 16 March 2018].

CTRL.blog, 2018. *EU GDPR and personal data in web server logs.* [Online] Available at: https://www.ctrl.blog/entry/gdpr-web-server-logs [Accessed 30 March 2018].

Datamation, c2018. *Structured vs. Unstructured Data.* [Online] Available at: https://www.datamation.com/big-data/structured-vs-unstructured-data.html [Accessed 20 March 2018].

Davis, B., 2017. *GDPR requires privacy by design, but what is it and how can marketers comply?*. [Online] Available at: https://www.econsultancy.com/blog/69376-gdpr-requires-privacy-by-design-but-what-is-it-and-how-can-marketers-comply [Accessed 25 March 2018].

Dbnetworks.com. (2018). [online] Available at: http://www.dbnetworks.com/pdf/DB-Networks-DBN-6300-Database-Discovery-Datasheet.pdf [Accessed 10 Apr. 2018].

EDPS, 2016. *Artificial Intelligence, Robotics, Privacy and Data Protection.* Marrakech, EDPS.

EU GDPR and personal data in web server logs. [online] Available at: https://www.ctrl.blog/entry/gdpr-web-server-logs [Accessed 13 Apr. 2018].

Gabel, D.D. & Hickman, T., 2017. Chapter 13: Cross-Border Data Transfers – Unlocking the EU General Data Protection Regulation. *White & Case*. Available at: https://www.whitecase.com/publications/article/chapter-13-cross-border-data-transfers-unlocking-eu-general-data-protection [Accessed April 9, 2018].

Good, T., 2018. *GDPR Data Breach Requirements.* [Online] Available at: https://datica.com/academy/gdpr-data-breach-requirements/ [Accessed 29 March 2018].

Globallegalpost.com (2018) How artificial intelligence can help solve GDPR issues. [online] Available at: http://www.globallegalpost.com/big-stories/how-artificial-intelligence-can-help-solve-gdpr-issues-22505427/ [Accessed 10 Apr. 2018].

Hall, R., 2017. *Is the Cloud Cheaper Than On-site Servers?*. [Online] Available at: https://www.silverlinesolutions.com/2017/01/cloud-cheaper-site-servers/ [Accessed 18 March 2018].

Hegde, Z., 2017. *GDPR compliance: We need to comply but where to begin?*. [Online] Available at: https://www.iot-now.com/2017/05/10/61469-gdpr-compliance-need-comply-begin/ [Accessed 02 April 2018].

Hendrix, C., c2017. *Why Your Company's Data is Important and Tips to Ensure Its Integrity.* [Online] Available at: https://www.bastiansolutions.com/blog/index.php/2013/08/16/tips-for-ensuring-data-integrity/ [Accessed 20 March 2018].

Inman, I., 2017. GDPR and the automotive industry. *Cox Automotive Data Solutions*. Available at: http://www.coxautodata.com/media/1310/blue-and-white-paper-3-gdpr-2017-12-07.pdf [Accessed April 10, 2018].

Lexology.com. (2018). Data security requirements under GDPR | Lexology. [online] Available at: https://www.lexology.com/library/detail.aspx?g=1426e18d-f687-45a0-b779-4aeb362a03ac [Accessed 10 Apr. 2018].

Lord, N., 2015. *What is Data Classification? A Data Classification Definition.* [Online] Available at: https://digitalguardian.com/blog/what-data-classification-data-classification-definition [Accessed 29 March 2018].

Lyster, A., 2017. Andrew Lyster. *Motor Trade News*. Available at: https://www.motortradenews.com/industry-news/41014-dealers-need-to-be-ready-for-gdpr-regulations [Accessed April 7, 2018].

Martin, J. A., 2018. *What is access control? 5 enforcement challenges security professionals need to know.*. [Online] Available at: https://www.csoonline.com/article/3251714/authentication/what-is-access-control-5-enforcement-challenges-security-professionals-need-to-know.html [Accessed 19 March 2018].

NADA, 2017. *Personal Data In Your Car,* U.S: National Automobile Dealers Association.

OnLineTech, c2018. *Public vs. Private Cloud Computing.* [Online] Available at: http://www.onlinetech.com/resources/references/public-vs-private-cloud-computing [Accessed 18 March 2018].

Pingidentity.com. (2018). General Data Protection Regulation (GDPR). [online] Available at: https://www.pingidentity.com/en/lp/secureGDPR.html [Accessed 9 Apr. 2018].

Quain, J. R., 2017. *Cars suck up data about you. Where does it all go?.* [Online] Available at: https://www.nytimes.com/2017/07/27/automobiles/wheels/car-data-tracking.html [Accessed 30 March 2018].

Rietti, B., c2017. *AUTOMATED REPORTING: FIVE BENEFITS FOR YOUR MARKET RESEARCH FIRM.* [Online] Available at: http://www.evancarmichael.com/library/benjamin-rietti/Automated-Reporting-Five-Benefits-for-Your-Market-Research-Firm.html [Accessed 01 April 2018].

Statista, 2016. *Revenue of the leading automotive manufacturers worldwide in FY 2016 (in billion U.S. dollars).* [Online] Available at: https://www.statista.com/statistics/232958/revenue-of-the-leading-car-manufacturers-worldwide/ [Accessed 11 April 2018].

Sybase Inc., c2009. *Ensuring Data Integrity.* [Online] Available at: http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.infocenter.dc00170.1510/html/iqapgv1/Intprot.htm [Accessed 18 March 2018].

Teeling, M., 2012. *What is Data Integrity? Learn How to Ensure Database Data Integrity via Checks, Tests, & Best Practices.* [Online] Available at: https://www.veracode.com/blog/2012/05/what-is-data-integrity [Accessed 19 March 2018].

10. Appendices

10.1 Appendix A

GDPR Articles:

Article 7 - Conditions for consent

Article 8 - Conditions applicable to child's consent in relation to information society services

Article 13 - Information to be provided where personal data are collected from the data subject

Article 17 - Right to erasure ('right to be forgotten')

Article 18 - Right to restriction of processing

Article 20 - Right to data portability

Article 32 - Security of processing

Article 33 - Notification of a personal data breach to the supervisory authority

Article 34 - Communication of a personal data breach to the data subject

Article 35 - Data protection impact assessment

Article 44 - General principle for transfers

Article 45 - Transfers on the basis of an adequacy decision

Article 46 - Transfers subject to appropriate safeguards

10.2. Appendix B

Group Work:

TEAM MEMBERS	Mobile Number	E-mail
1. Aaruni	17200419	aaruni.bhugul@ucdconnect.ie
2. Ankita	17204239	ankita@ucdconnect.ie
3. Chinmay	17201526	chinmay.kuchya@ucdconnect.ie
4. Prashik	17200040	prashik.chitkesiwar@ucdconnect.ie
5. Sherin	17200643	samuel.varghese@ucdconnect.ie

INFORMAL COMMUNICATION

We have decided

1) To make a WhatsApp group so that we can communicate our ideas to all members of the group at any time.
2) To create a google drive so that we can upload of finished pieces of work so that all team members can read and review them.

MEETINGS

We have decided

1) To meet on a regular basis and for each team member to have their work completed for each meeting.

MAKING DECISIONS

We have agreed

1) To split the project up into sections and assign a group member to each section.
2) All members of the group will examine and edit the final draft.

SANCTIONS

We hope to work in harmony together. We have different strengths. We accept that this is a group piece of work and we are all responsible for doing our best. However, we agree that

- If individuals have difficulties in working with the team or on the task, we will try to sort them out promptly by talking with each other
- We will seek advice - as soon as is possible - from our tutor for those serious problems which we cannot resolve ourselves.

SIGNED

Planning Activities:

Jobs List	
What needs doing?	***Who will do it?***
Introduction to GDPR	Ankita
Impact and challenges of GDPR	Prashik
Infrastructure Planning	Sherin
Implementation of Solution	Aaruni
Recommendations and Conclusion	Chinmay
Presentation	All Team members