

GDPR and Vergic – an overview

Table of Contents

1	INTRODUCTION.....	2
1.1	USEFUL INFORMATION AND LINKS	2
2	BASIC DEFINITIONS – DATA CONTROLLER AND DATA PROCESSOR	2
2.1	DATA PROCESSOR.....	2
3	BASIC DEFINITIONS – PERSONAL RECORD	2
3.1	WHAT IS A PERSONAL RECORD?	2
3.2	VERGIC ENGAGE PLATFORM (VEP) AND PERSONAL RECORDS	3
4	RESPONSIBILITY AND ACCOUNTABILITY	3
5	CONSENT	4
6	PRIVACY BY DESIGN AND BY DEFAULT	5
7	RIGHT TO ERASURE	5
8	DATA PORTABILITY	5
9	CERTIFICATION.....	5

1 INTRODUCTION

The purpose of this document is to give a brief overview of the GDPR from a Vergic perspective. This is by no means a complete analysis of all possible consequences but it will point out the key areas where action is needed (and taken) either by Vergic or together with our Customer.

Each chapter gives a general outlook/overview on the specific topic and then, at the end it lists or describes measures and actions taken by Vergic or, in some cases actions needed also by our Customer

1.1 Useful information and links

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

<http://computersweden.idg.se/2.2683/1.657438/eu-nya-regler-foretag>

<http://www.datainspektionen.se/lagar-och-regler/eus-dataskyddreform/forberedelser-for-personuppgiftsbitraden/>

2 BASIC DEFINITIONS – DATA CONTROLLER AND DATA PROCESSOR

Vergic will always in relationship to a Customer be the Data Processor (“personuppgiftsbiträde”), and our Customer the Data Controller. Already, as of today Vergic most often sign a Data Processing Agreement (DPA) as part of a contract.

2.1 Data processor

As mentioned above this role is already existent but with GDPR it will carry more obligations. Information below is condensed, see more detailed information under the link regarding “personuppgiftsbiträde” in the introduction. When setting up a contract with the Customer we will be the Data processor and sign as such party but when doing the contract through a partner Vergic will probably (but not necessarily) have a role as a sub processor.

The Customer (Data Controller) has the responsibility to define and justify what type of personal data that shall be processed and possibly stored. When setting up the DPA all categories of processing that is supposed to be done on behalf of the controller (Customer) by the Data processor (Vergic) will be defined in the DPA.

Vergic commitments and actions

- To Keep a record of all categories of processing that is done on behalf of the controller as defined in the DPA
- Appoint a Data Protection Officer (DPO). Not always applicable for a Data Processor, only applicable in some cases but as we are processing data on behalf of Public Authorities we will (and already have) appointed a DPO

3 BASIC DEFINITIONS – PERSONAL RECORD

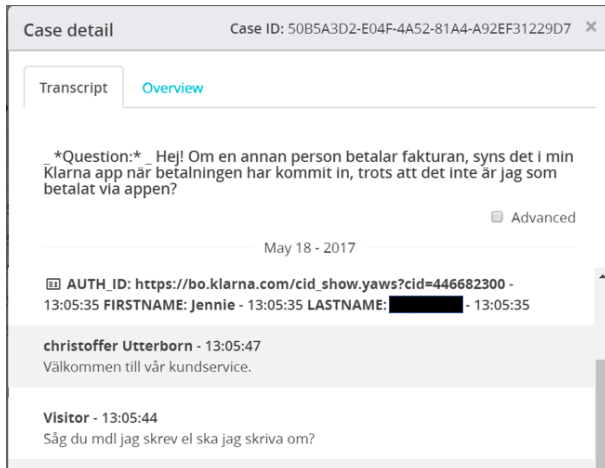
3.1 What is a personal record?

(In Swedish, definition from the Swedish Data Protection Authority)“Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller on-lineidentifikatorer eller en eller flera faktorer

som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet” (Datainspektionen).

3.2 Vergic Engage Platform (VEP) and personal records

Example below is with an authenticated Customer



In this example it is actually not really clear if we store a personal record or not (last name blanked). The authentication ID itself cannot identify the end Customer since you need to match it in the Customers database. We do have first name and last name.

In Germany personal record has been defined as a group <4, i.e. in most cases this would not be a personal record without other “markers” in the transcript. However, with a very unusual name it would probably be considered being a personal record.

Conclusion:

- A chat transcript with only first name or a “normal” last name would not be a personal record whereas a transcript with a very unusual name might be considered being that
- The IP-address, however debated shall also be seen as a personal record
- If the authentication ID like a social security number, such as our public Customers it would always be a personal record. However, in the case above the Auth. ID is not possible to connect to an ID in the Vergic Database

Vergic commitments and actions

To keep it simple and to avoid any tricky interpretations with regards to GDPR if a record is to be defined as personal data or not the Vergic policy and principal rule is that we always deal with and store personal data.

4 RESPONSIBILITY AND ACCOUNTABILITY

This is mainly a responsibility of the Data Controller, to justify why, to show the purpose etc. of processing personal data. However, as a Data processor one important matter is that Vergic has to be able to support the specific data retention policy that the Data Controller – our Customer will have.

As a Data Processor Vergic is responsible and accountable for not only fulfilling the commitments we carry out on behalf of the Data Controller, Vergic must also be able to show how and what measures that has been taken to protect data. This falls under the responsibility of the DPO.

Vergic commitments and actions

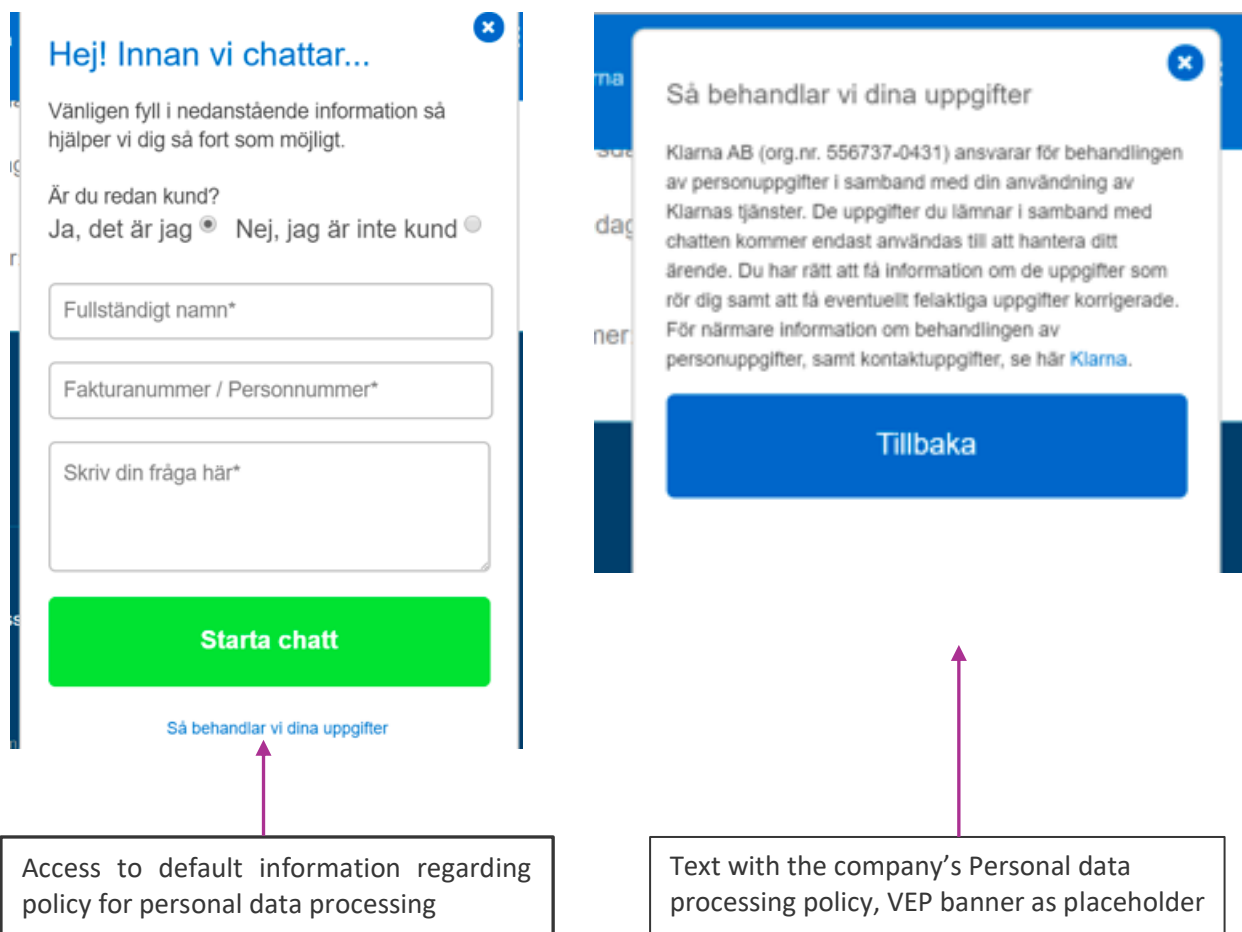
Besides that is mentioned above development is taking place and will be implemented well in time before GDPR begins to apply. This will allow:

- To set a retention policy per account i.e. per Customer

- To make this even more granular by implementing tools to do this on a per case type or even per case basis
- Measures and actions taken under chapter 6, Privacy by design and by default

5 CONSENT

Consent must be given for the purposes for which data is collected and used. The Data Controller must be able to prove consent. This is the Controllers (Customers) obligation but Vergic will be able to support our Customer on this matter. This can be done as illustrated below:



Access to default information regarding policy for personal data processing

Text with the company's Personal data processing policy, VEP banner as placeholder

The definition of “prove consent” is somewhat unclear, but for the moment we assume that it will be enough to say in writing “by starting this chat I give consent...”

Vergic commitments and actions

See above, to offer different types of placeholders where the personal data processing policy can be presented and consent can be given. If the Data Controller wishes to store each individual consent Vergic does not provide a solution for that, we only provide the placeholder as described above.

6 PRIVACY BY DESIGN AND BY DEFAULT

Pseudonymisation is a key component of this. The way Vergic, as a Data Processor works with pseudonymisation is by encryption.

Vergic commitments and actions

Through the new Architecture (already implemented) all databases, both production databases and backups are encrypted. All traffic is transmitted over the https protocol.

7 RIGHT TO ERASURE

The individual has the right to request erasure on a number of grounds, that is part of the relationship between the end Customer and our Customer, the Data Controller. The type of data that an end customer typically would want to erase would reside in a CRM system or equivalent. In most cases this is not applicable to the type of data Vergic stores.

However, if an end customer wants to erase any possible personal data that might reside in a chat transcript that is also possible but the record cannot be retrieved by name. Vergic does not store any personal records in that format, it only resides as running text in a transcript. It has to be searched by date.

Vergic commitments and actions

Possibility to erase a specific chat transcript

8 DATA PORTABILITY

Phrased as:

“A person shall be able to transfer their personal data from one electronic processing system to and into another, without being prevented from doing so by the data controller. In addition, the data must be provided by the controller in a structured and commonly used open standard electronic format”.

This is technically possible but Vergic does not see it as applicable to us as being the type of Data processor we are.

9 CERTIFICATION

There will be some sort of GDPR certification, there are no details on this at this time.

Vergic commitments and actions

Monitor the subject, if applicable undergo future certification.