Bech·Bruun

Copenhagen, December 2019

DPO Audit DrugStars ApS

The Data Controller
DrugStars ApS (“DrugStars”)
Emdrupvej 28 A, 4.
2100 København Ø
CVR-no.: 36 89 39 74

Subject
DPO Audit

Data Protection Officer (DPO)
Bech-Bruun Law Firm P/S
CVR-no.: 38 53 80 71
Langelinie Allé 35
2100 Copenhagen
Denmark

Table of contents

Appendix

Appendix 1: Request list/questions regarding records, data processors, data breach, security, legal basis and duty to provide required information.

1. Introduction

As part of the DPO-service agreement, Bech-Bruun has as data protection officer ("DPO") completed the yearly audit ("DPO Audit") of DrugStars.

The purpose of the DPO Audit is to control DrugStars' compliance with the General Data Protection Regulation ("GDPR"), the Danish Data Protection Act ("DDPA") and related practices from the Data Protection Authorities (together the "Data Protection Rules").[1]

The DPO Audit is prepared in accordance with the requirements of the GDPR for the auditing to be performed by Bech-Bruun in the role as DPO for DrugStars. The DPO Audit is thus performed on the risk-based approach as stipulated in the GDPR. This implies that the DPO Audit only includes audit of selected processing areas at DrugStars. The Processing areas chosen relates to DrugStars processing of personal data on customers in the DrugStars App (collectively referred to as "Customer Data").

The result of the completed DPO Audit serves as a basis for the reporting to DrugStars' top management team.

1.1 Selected areas

For DrugStars the following areas of processing have been chosen for the DPO Audit in relation to Customer Data:

1. **Records**
   DrugStars' compliance with the obligation to keep records of their processing of personal data (GDPR article 30).
2. **Data processors**
   DrugStars' compliance with the obligation to enter into data processing agreements, the content of the data processing agreements and DrugStars' audit of the data processors used (GDPR article 28).
3. **Data breach**
   DrugStars' management of personal data breaches along with any follow-up measures and awareness activities (GDPR articles 32, 33 and 34).
4. **Security**
   DrugStars' management of the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the identified risk (GDPR article 32).
5. **Legal basis**
   DrugStars' management of the obligation to ensure the necessary legal basis to process

[1] Data Protection Regulation article 39 (2). The obligation to monitor compliance (control of the data controller) is subsequent to article 5 (2), 24 and 39 (1) of the Data Protection Regulation.

personal data (GDPR articles 5 (1) (a), 6, 9, 10, 11 and the DDPA §§ 6, 78, 9, 10, 11, 12 and 13).

6. **Information to be provided**
DrugStars' management of the obligation to properly inform the customers about DrugStars' processing personal data (GDPR article 13 and 14 and DDPA §§ 22 and 23).

1.2 Basis for DPO Audit

The review of each of the abovementioned processing areas in relation to the Customer Data have been based on:

A. DrugStars' answers to a request-list/questionnaire prepared by the DPO and material that DrugStars was asked to submit to the DPO. The request-list/questionnaire forwarded and answered by DrugStars, is enclosed as appendix 1 to this report.

B. Interviews with selected employees performed on September 25, 2019:

- Claus Møldrup, Chief Executive Officer
- Bilquees Kustagi, Chief Operating Officer

C. Spot checking if data processing agreements are prepared in accordance with article 28 of the GDPR.

D. Assessment of whether written policies, procedures, guidelines and information material are available.

1.3 Methodology of the DPO Audit report

Based on our control of the selected processing areas in relation to Customer Data cf. section 1.1 above, we have prepared an overview of our most important observations and if relevant recommendations for measures that DrugStars should initiate with a view to increase the compliance level going forward.

Our summary is provided in section 2 below and a more detailed list is provided in section 3 below. The list contains an indication of the relevant area, description of the observations, our recommendation along with a specification of the compliance level indicated by the traffic light principle (red, yellow and green).

1.3.1 Explanation of compliance level

Compliance level	Explanation
	Compliance level is in violation of the Data Protection Rules. Non-compliance may result in a fine.
	Compliance level is in violation of recommendations laid down by the Data Protection Agency and/or other relevant authorities. Non-compliance may result in criticism/warning.
	Compliance level is in accordance with the Data Protection Rules.

2. Summary of observations and recommendations

The result of the completed DPO Audit shows that DrugStars has implemented sufficient measures to ensure compliance in relation to the processing of Customer Data. In general, DurgStars has a very high level of compliance in relation to the Data Protection Rules concerning the processing of Customer Data.

The more detailed list is available in section 3 below.

3. Elaboration of observations

1.	Records of processing	
Number	**Observation**	**Level**
1.1	DrugStars has prepared a written record for processing Customer Data in accordance with article 30 (1) of the GDPR.	
2.	**Data processors**	
Number	**Observation**	**Level**
2.1	**Data processing agreements** DrugStars has entered into data processing agreements with all companies that process Customer Data on behalf of DrugStars (data processors) in accordance with article 28 of the GDPR. At the interview on September 25, DrugStars confirmed that all data processing agreements in relation to Customer Data have been entered into.	
2.2	**Audit and documentation of data processors** DrugStars has established when and how the data processors will be audited. Additionally, DrugStars has prepared a written procedure describing which person is responsible for entering into new data processing agreement.	
3.	**Data breach**	
Number	**Observation**	**Level**
3.1	**Data breach policy** DrugStars has prepared a data breach policy that consists of (i) a data breach response plan flow (ii) data breach response plan template (iii) where a data breach is reportable (v) and communication to affected data subjects. The data breach policy contains information of roles and responsibilities, deals with the definition of security breaches, concrete examples of typical security breaches, explains how employees	

	must act in the event of a potential security breach, when, to whom and how a security breach must be reported to the Danish Data Protection Agency, how a security breach must be documented and when data subjects must be informed of the security breach.	
3.2	**Awareness of data breaches** DrugStars has created awareness of possible data breaches pursuant to the Data Protection Rules through training of employees, forwarded policies and posters at the office. DrugStars has informed us that no data security breaches have occurred so far.	
4.	**Security**	
Number	**Observation**	**Level**
4.1	**Technical security measures** DrugStars has implemented a high level of technical security in relation to the processing of Customer Data. DrugStars has informed us that the DrugStars App ensures that all Customer Data is encrypted in accordance with the guidelines from the Danish Data Protection Agency. Additionally, DrugStars ensures that new systems, services and technical solutions etc. comply with the principles of privacy by design and privacy by default. Furthermore, the principles of pseudonymisation, transparency, data minimisation, anonymisation, and automatic deletion routines have been implemented in relation to the Customer Data. In conclusion, it is our assessment that DrugStars' current technical solutions and set-up ensure a level of security appropriate to the risk. Our observation is only based on the documentation provided by DrugStars. We have not tested DrugStars' technical security in practice.	
4.2	**Organisational security measures** In general, DrugStars has implemented a high level of organisational security, including training of employees about data breaches, access restrictions, authorisations, and passwords. In addition, DrugStars has implemented a comprehensive IT policy for employees. Employee training of	

	the Data Protection Rules is part of the DPO-service and is carried out each year.	
5.	**Legal basis**	
Number	**Observation**	**Level**
5.1	DrugStars refers to the proper legal bases for the processing of both non-sensitive personal data and sensitive personal data. When required to, DrugStars obtains prior consent separate from other documents as part of the flow through the App. Consents are obtained in accordance with the Data Protection Rules and the guidelines from the Data Protection Authorities. The proper legal bases are both documented in the privacy policy and the records of processing activities.	
6.	**Duty to provide required information**	
Number	**Observation**	**Level**
6.1	DrugStars has prepared a general privacy policy named “Policy on Data Privacy”. The privacy policy provides the required information to the customers in accordance with article 13 and 14 of the GDPR. The privacy policy is actively provided to the Customers as part of the sign-up flow and may subsequently be located by the customer through the App.	

---o0o---

Copenhagen, December 2019

Susanne Stougaard, Partner

Nilas Monberg, Associate