Advokatfirma
DLA Piper Norway DA
Bryggegata 6
Postboks 1364 Vika
N-0114 Oslo
Norway

T +4724131614
F +4724131501
W www.dlapiper.no
NO 982 216 060 VAT-registered

SuperOffice
On behalf of: Chief Product Officer Guttorm Nielsen

Your reference

Our reference

Oslo, 23 March 2018
Lawyer responsible:
Jan Sandtrø

GDPR COMPLIANCE, SUPEROFFICE CRM

I refer to the request for an assessment of SuperOffice CRM in relation to the requirements of the Norwegian Personal Data Act and the General Data Protection Regulation (GDPR) and subsequent meetings to exchange information and review functionality and forwarded documentation.

We have conducted a review of SuperOffice CRM and consider that SuperOffice CRM has the necessary functionality to ensure that organisations using SuperOffice CRM can adhere to the requirements of the General Data Protection Regulation (GDPR). Reference is made to the enclosed detailed assessment.

Yours sincerely,
Advokatfirma DLA Piper Norway DA

Jan Sandtrø
Lawyer/Partner
Jan.Sandtro@dlapiper.com

ENCLOSURES

1. PROCESSING

Data minimisation	
Assessment topic:	Whether more personal data is being processed than is necessary.
Assessment:	Approved
Remarks:	Based on our assessment, no more data than necessary is being processed by SuperOffice CRM, and the system gives users the option to adapt the data that is acquired and processed.
Action required:	None

Free-text fields	
Assessment topic:	Whether free-text fields are checked for processing.
Assessment:	**Approved**
Remarks:	The solution contains free-text fields, and the controller (the customer) must ensure that the general requirements of the regulations are adhered to in relation to the use of free-text fields.
Action required:	Consideration may be given to the inclusion of a notification that users must be wary of entering personal data in free-text fields.

Purpose	
Assessment topic:	Whether personal information is being processed to an extent which exceeds the purpose for which it was acquired.
Assessment:	**Approved**
Remarks:	The solution does not involve the processing of personal data to an extent which exceeds the purpose for which it was supplied; however, this is something that the controller (the customer) must ensure does not happen in relation to the purposes for which the customer uses the solution.
Action required:	None

Legal basis for processing	
Assessment topic:	Whether there is a legal basis for all processing of personal data.
Assessment:	**Approved**
Remarks:	Whether there is a legal basis for the processing of personal data in SuperOffice CRM is an issue that must be assessed and addressed by the controller (the customer). If consents, contracts, legal grounds or the protection of vital interests pursuant to Article 6 of GDPR are used, the controller must also assess whether the basis for the processing is adequate for the processing performed by SuperOffice CRM.

	SuperOffice CRM contains functionality to ensure that the customer can assess whether there is a basis, and the customer can adopt the relevant basis associated with the individual functionality. In addition, there is a solution for obtaining consent which can be configured according to the scope of the consent (which also ensures the granulation of consent, i.e. the division of the consent in relation to the individual circumstance for which consent is being given). Documentation of the consent is ensured by registering the scope of the consent for an individual data subject and by registering the time at which the data subject gives their acceptance and the values entered in the form. This also ensures a double opt-in for verification of the data subject in relation to an e-mail address. SuperOffice CRM can also be configured to ensure that no direct marketing takes place via e-mail or text message without a legal basis to ensure compliance with the regulations.
Action required:	There should be improved functionality to ensure that the consent text is documented.

Specific categories of data	
Assessment topic:	Whether there is a basis for the processing of specific categories of personal data, including data relating to criminal offences.
Assessment:	**Approved**
Remarks:	Whether or not specific categories of data can be processed is an issue for the controller (the customer) to decide. However, the solution makes no provision for the storage and processing of specific categories of data in the solution (besides the free-text fields, see above), but the controller can add traps to detect specific categories of data and lock these for special use.
Action required:	None

Deletion	
Assessment topic:	Whether personal data is deleted when it is no longer required or when there is no basis for the processing.
Assessment:	**Approved**
Remarks:	The solution enables the controller to fulfil the requirements for deletion in accordance with the regulations, and there is a facility for routine deletion without this having to be done manually. Actual deletions must take place in the solution (information must not be set to 'passive'). Information may also be marked for deletion, with actual deletion taking place following an expiry period. It is possible to delete information according to specific criteria associated with individuals (this functionality was not in place at the time of the review, but will be in place by 25 May according to SuperOffice). It is possible to retain information associated with legal entities, even if the information relating to private individuals has been deleted. It is also possible to retain information for statistical purposes with the removal of personally identifiable information in cases where there are grounds for processing such information.

	SuperOffice CRM has functionality for deletion when the purpose no longer applies, such as in the case of inactivity or a specific purpose (such as for a project that has been completed), the withdrawal of consent, objection to the processing or because deletion must be carried out in order to fulfil a legal obligation.
Action required:	None

2. PROCESSORS

Processor agreement	
Assessment topic:	Processor agreements have been established in accordance with GDPR with all processors, including between group companies, and where the company is the processor.
Assessment:	**Approved**
Remarks:	SuperOffice CRM is covered by its own processor agreement between SuperOffice and the controller (the customer).
Action required:	None

Sufficient guarantees	
Assessment topic:	Whether the processor satisfies the requirements for information security.
Assessment:	**Not assessed**
Remarks:	SuperOffice is the processor in the cloud solution for SuperOffice CRM. We have not assessed whether SuperOffice and personal data processed therein fulfil the requirements regarding information security, i.e. sufficient organisational and technical measures are in place to ensure compliance with the rules. However, SuperOffice practices transparency in relation to security, and information is available on its website: https://www.superoffice.com/trust-center.
Action required:	An assessment can be made by experts within information security.

Subcontractors (sub-data processors)	
Assessment topic:	Whether processor agreements have been established with subcontractors processing personal data as subcontractors.
Assessment:	**Approved**
Remarks:	SuperOffice has established processor agreements with all suppliers processing personal data for controllers (customers).
Action required:	None

3. RIGHTS OF THE DATA SUBJECT

Information obligation	
Assessment topic:	Whether sufficient information has been provided to employees, customers and other persons registered regarding the personal data being processed.
Assessment:	**Approved**
Remarks:	The information obligation rests with the controller (the customer), but the processor must provide assistance regarding the fulfilling of this obligation. SuperOffice CRM provides functionality to allow controllers to fulfil some of the obligations under GDPR, including information relating to employees, supervision, correction and deletion, and in particular the information obligation in accordance with Articles 12-15, which is ensured by sending e-mails.
Action required:	None

Automation and profiling	
Assessment topic:	Whether any automation has a legal basis and is being implemented in accordance with the rules.
Assessment:	**Approved**
Remarks:	The solution does not involve any automation.
Action required:	None

Corrective actions and updating	
Assessment topic:	Whether measures are in place to ensure that personal data is accurate and updated.
Assessment:	**Approved**
Remarks:	The information is provided by the controller (the customer), who must correct or update it themselves. The information in the solution can also be 'cleansed' in relation to public lists via partners.
Action required:	None

Right to object and right to restrict processing	
Assessment topic:	Whether objections and the right of data subjects to restrict the processing that is carried out are complied with.
Assessment:	**Approved**
Remarks:	This is a requirement which is imposed with respect to the controller (the customer) and which the processor must be made particularly aware of. SuperOffice CRM will support limited processing by provisionally transferring selected information to another system (i.e. moving to a more screened system) and by making certain personal information (such as individual fields) inaccessible to users (individuals or groups). It is also possible to specify in the system that personal data relating to a person is restricted.
Action required:	None

Right of access	
Assessment topic:	Whether the right of access is being and can be complied with.
Assessment:	**Approved**
Remarks:	The right of access for data subjects has been met through individual access to data or through provision for the submission of requests for access to the controller (the customer). Arrangements have been made for the controller to provide details of the information being processed in a simple manner by generating a report on the processing that is carried out. The access and shielding can be adequately configured to ensure confidentiality, but there is no functionality to screen individual fields; this will be developed later (but not until after 25 May).
Action required:	Screening of individual fields should be incorporated into the solution.

4. INFORMATION SECURITY AND IT SYSTEMS

Control of access / shielding	
Assessment topic:	Whether more people have access to the data than is necessary.
Assessment:	**Approved**
Remarks:	SuperOffice CRM meets the requirements to allow access to personal data to be restricted.
Action required:	Limit access of other companies and ensure screening of specific categories of personal data.

Privacy by design	
Assessment topic:	Whether IT systems support privacy by design/default.
Assessment:	**Approved**
Remarks:	As follows from the other assessments, SuperOffice supports the requirements for privacy by design/default.
Action required:	None (subject to the measures proposed elsewhere in the review)

Certification and codes of conduct	
Assessment topic:	Whether existing codes of conduct and certification are being followed and adhered to.
Assessment:	**Not applicable**
Remarks:	There are currently no codes of conduct or certification schemes for solutions in SuperOffice CRM.
Action required:	None

Data breaches and notification	
Assessment topic:	Whether data breaches are handled as required, including whether notification takes place as stipulated in the event of a data breach.
Assessment:	**Approved**
Remarks:	SuperOffice has routines to ensure that the controller (the customer) is notified within the required time and that the notification is regulated in the processor agreements with the processors. The procedures handle notifications, both in cases where notification of a breach is received from a data subject and when it is detected by SuperOffice. Procedures may also be established for notifying the Norwegian Data Protection Authority and data subjects where the controller so requires.
Action required:	None

Data portability	
Assessment topic:	Whether IT solutions and systems support data portability.
Assessment:	**Approved**
Remarks:	Data portability is unlikely to be relevant to SuperOffice CRM, but the solution allows for this in connection with the export of data should data portability be required.
Action required:	None
Training	
Assessment topic:	Whether employees have received adequate training concerning the processing of personal data.
Assessment:	**Approved**
Remarks:	Training regarding the processing of personal data is provided in SuperOffice and the requirements for routines also follow the quality systems that have been implemented.
Action required:	None

5. TRANSFERS

Transfers to other controllers/third parties	
Assessment topic:	Whether there is a basis for the transfer of personal data to other controllers and whether it is ensured that such parties delete data if required.
Assessment:	**Approved**
Remarks:	SuperOffice does not transfer data to third parties unless such transfers follow from instructions issued by the controller (the customer). Whether the transfer may be performed in accordance with the customer's instructions depends on whether the customer has a basis for the transfer.
Action required:	None

Transfers to third countries	
Assessment topic:	Whether there is a basis for the transfer of personal data to third countries.
Assessment:	**Approved**
Remarks:	SuperOffice does not transfer personal data that is being processed for the controller (the customer) to third countries, i.e. countries outside the EEA.
Action required:	None