AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500
autoriteitpersoonsgegevens.nl

INSOLAD
Attn. the board
Dorp 53
3415 PC POLSBROEK

Date
6 January 2020

Our reference
z2019-12871

Contact person
070 8888 500

Subject
The processing of personal data in the event of liquidation

Dear board,

The Dutch Data Protection Authority (DPA) draws your attention to the following.

Introduction

In this letter, the Dutch Data Protection Authority (DPA) outlines the legal framework with regard to the processing of personal data by insolvency practitioners. Through INSOLAD, the Dutch Data Protection Authority (DPA) aims to inform as many insolvency law lawyers and (prospective) insolvency practitioners as possible of the legal framework that applies to the processing of personal data in the estate of a bankrupt person or liquidated legal entity, and of the responsibility for compliance with the GDPR that rests with the insolvency practitioner in that context.

The Dutch Data Protection Authority (DPA) considers it very important that this subject is brought to the attention of your members and prospective members, partly in view of the number of liquidations that are ordered every month in the Netherlands (November 2019: 284 companies and institutions put into liquidation[1]) The Dutch Data Protection Authority (DPA) therefore request that you bring the contents of this letter to their attention.

Please inform the Dutch Data Protection Authority (DPA) whether you comply with this request.

[1] 1 This is the figure most recently published by Statistics Netherlands. The stated figure has been corrected for court session days and excludes sole proprietorships. See: https://www.cbs.nl/nl-nl/nieuws/2019/50/aantal-faillissementen-neemt-toe.

Date
6 January 2020

Our reference
z2019-12871

Applicability of GDPR in the event of liquidation

In almost every liquidation, the estate includes personal data, such as customer files, membership files and personnel files on analogue or digital data carriers. 'Personal data' means: all information on an identified or identifiable natural person (the 'data subject').[2][3] Personal data must be handled with care, also in the event of liquidation.

The GDPR contains rules that aim to ensure that the rights and freedoms of data subjects are protected in the context of the processing of personal data. These rules also apply to the processing of personal data by insolvency practitioners. Insolvency practitioners, in their capacity as controller, are obliged to comply with the rules in the GDPR and the General Data Protection Regulation (Implementation) Act (in Dutch: UAVG).

The Dutch Data Protection Authority (DPA) monitors compliance with these rules in the Netherlands and can take enforcement action in the event of violations.

Management summary

The most important parts of this letter are set out below.

• The insolvency practitioner, in his capacity as controller, is responsible for compliance with the GDPR;
• In this context, the insolvency practitioner has a duty of accountability (Article 5, paragraph 2, GDPR);
• The insolvency practitioner must process personal data on the basis of a legally valid basis within the meaning of Article 6 GDPR, limited to what is necessary for the purposes for which they are being processed.
• Special conditions apply to the processing of special categories of personal data or personal data concerning criminal convictions and criminal offences and the citizen service number.
• Personal data must be collected for specified, explicit and legitimate purposes and not further processed by the controller in a manner that is incompatible with the purpose of collection ('purpose limitation principle'). Specific rules apply for (intended) further processing of personal data for other purposes.
• Another controller cannot (further) process personal data based on the legal basis of the controller who collected the personal data.
• The provision of personal data by the insolvency practitioner to another controller, for example, in the context of realisation of the estate, cannot take place on the basis of compatibility with the collection purposes.
• In the context of the continuation of (the activities of) the same liquidated legal entity by the insolvency practitioner, the processing of already lawfully processed personal data can in principle continue to take place on the basis of the original legal basis or bases.

[2] Personal data can form an analogue (e.g. on paper) or digital (e.g. on a server) part of the estate.
[3] See Article 4 (1) General Data Protection Regulation (GDPR). An identifiable natural person is one who can be identified, directly or indirectly, in particular on the basis of an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

• If the contract takeover takes place lawfully, in compliance with all applicable rules, the personal data necessary for the contract takeover can be transferred to the new contracting party. The insolvency practitioner can in principle provide the personal data necessary for the performance of the contract to the new contracting party on the basis of Article 6, paragraph 1, under b, GDPR.
• Personal data can only be sold on the basis of the prior consent of the data subject(s) in accordance with Article 7 GDPR.
• If an insolvency practitioner wishes to monetise equipment, including digital data carriers (e.g. in computers or laptops), the insolvency practitioner must ensure that the equipment does not or no longer contains any data carriers or that the personal data on the relevant data carriers are irreversibly destroyed before the equipment is disposed of.
• After a legal entity has ceased to exist due to dissolution, it will be necessary to determine what personal data have remained in the estate, what should be done with those personal data and who is responsible for those personal data in that context.
The previous points will be further elaborated in the remainder of this letter.

Insolvency practitioner is controller
A controller is subject to various obligations to protect personal data . A controller is a natural person or legal entity, a public authority, agency or another body which, alone or jointly with others, determines the purpose and means of the processing of personal data.[4]

'Processing' is a broad concept. It includes an operation or set of operations with regard to personal data or sets of personal data, whether or not carried out by automated processes, such as collecting, recording, organising, structuring, storing, updating or modifying, retrieving, consulting, using, providing by means of transmission or otherwise making data available, aligning or combining, shielding, erasing or destroying them.[5]

Under the liquidation order, the debtor automatically loses the disposal and administration of the assets that form part of the liquidation.[6]

The liquidation includes all assets of the insolvent company at the time of the liquidation order and anything acquired during the liquidation.[7] Under the Bankruptcy Act, the insolvency practitioner is charged with the administration and liquidation of the estate of a company in liquidation.[8] The charge of administration and liquidation implies actual power and control over the insolvent company's estate, also considering the fact that only the insolvency practitioner can legally bind the insolvent company assets in liquidation.[9] The position of the insolvency practitioner(s) is therefore accompanied by a (joint or otherwise) responsibility with regard to the personal data in the estate of the insolvent company.

[4] 4 See Article 4 (7) GDPR.
[5] 5 Article 4 (2) GDPR.
[6] See Article 23 Bankruptcy Act (Fw).
[7] Article 20 Bankruptcy Act. See also Article 24 Bankruptcy Act.
[8] See Article 68 (1) Bankruptcy Act.
[9] See Article 25 (1) Bankruptcy Act.

In the context of the settlement of the liquidation on the basis of Article 137c of the Bankruptcy Act, the insolvency practitioner must proceed to realise the estate. The insolvency practitioner is authorised to dispose of goods.[10] This will often mean that assets falling within the estate will be sold.[11] It is important to realise that the assets in question may contain personal data, and that disposal of personal data generally involves processing those personal data.[12]

Lawfulness, fairness and transparency of the processing

From the moment an insolvency practitioner is appointed as administrator of an estate, the insolvency practitioner is responsible for compliance with the GDPR with regard to personal data processed in the context of the administration and liquidation of the estate and more in general with regard to processing operations for which the insolvency practitioner qualifies as a controller.

Among other things, being a controller means that an insolvency practitioner is responsible for the lawful, fair and transparent processing of the personal data in question.[13]

Lawfulness

Personal data may only be processed by the insolvency practitioner if and to the extent that the processing is based on a legal basis within the meaning of Article 6 GDPR, limited to what is necessary for the purposes for which they are processed.

In addition, additional requirements must be met in the event of the (intended) processing of special categories of personal data [14] or personal data relating to criminal convictions and criminal offences.[15] The citizen service number (Dutch: BSN) are also personal data with a high degree of sensitivity.

For example: In principle, a ban applies with regard to the processing of special categories of personal data. This means that a controller may not process the categories of personal data referred to in Article 9(1) GDPR , unless the controller can invoke a ground for exception within the meaning of Article 9(2) GDPR with regard to the personal data in question.

[10] Article 101 (1) Bankruptcy Act.
[11] See also Article 175 Bankruptcy Act.
[12] In this letter, the Dutch Data Protection Authority (DPA) limits itself to an observation from a data protection perspective. In this letter, the Dutch Data Protection Authority (DPA) does not comment on whether personal data can be included under the concept of 'assets' within the meaning of Article 20 of the Bankruptcy Act, as part of the estate to be administered and settled by the insolvency practitioner. The Dutch Data Protection Authority (DPA) notes that this has been discussed in the literature and it has been argued several times that personal data cannot be qualified as either a thing or a good. What is certain, however, is that data can be valued in money and are considered part of the estate. Practice shows that insolvency practitioners sell personal data. This raises the question of whether the alienation of personal data by an insolvency practitioner is in accordance with Article 5(1)(a) GDPR in appropriate cases. In his capacity as a controller, an insolvency practitioner must, among other things, be able to demonstrate the lawfulness and fairness of the processing of personal data within the meaning of Article 5(2) GDPR ('accountability').
[13] See also Article 5 GDPR.
[14] Special categories of personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and processing of genetic data, biometric data for the purpose of uniquely identifying a person, or data concerning health, or data relating to a person's sexual behaviour or sexual orientation.
[15] See Articles 9 and 10 GDPR and Articles 22 et seq. and 31-33 UAVG.

'Lawfulness' in Article 5(1)(a) GDPR means that, more generally, the processing of personal data must take place in accordance with the applicable laws and regulations, including the GDPR and UAVG.

Further processing for other purposes
Personal data must be collected for specified, explicit and legitimate purposes and not further processed by the controller in a manner incompatible with the purpose for which they were collected ('purpose limitation principle').[16] Usually, the personal data will have been collected by the insolvent legal entity. In certain cases, an insolvency practitioner may wish to further process personal data for purposes other than those for which the personal data were initially collected by the insolvent legal entity. Specific rules apply for (intended) further processing of personal data for other purposes.

Pursuant to Article 6(4) GDPR, personal data (e.g. the customer base of the insolvent legal entity) may be further processed by the controller for purposes other than the purposes for which the personal data were initially collected, if and insofar as:

(i) the data subjects have given their consent[17] for this;
(ii) there is a specific statutory obligation or statutory authority that constitutes a necessary and proportionate measure to safeguard the objectives referred to in Article 23(1) GDPR; or
(iii) it concerns so-called 'compatible processing'.

When assessing whether intended further processing is compatible with the collection purposes, the following factors, among others, must be taken into account:

a) any connection between the purposes for which the personal data were collected and the purposes of the intended further processing;
b) the context in which the personal data were collected, in particular as regards the relationship between the data subjects and the controller;
c) the nature of the personal data, in particular whether special categories of personal data are processed and whether personal data relating to criminal convictions and criminal offences are processed;
d) the possible consequences of the intended further processing for the data subjects;
e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.[18]
f) If further processing for other purposes is compatible with the purposes for which the personal data were initially collected, there is no separate legal basis for that specific further processing, other than the one by virtue of which the collection of personal data was allowed.[19]

Note: A controller must have its own legal basis within the meaning of Article 6 (1) GDPR to be allowed to process personal data. Another controller cannot (further) process personal data based on the legal basis of the controller who collected the personal data from the data subject or otherwise. This does not rule out

[16] Article 5 (1)(b) GDPR.
[17] For the conditions for consent, see Article 7 GDPR. See also: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf.
[18] See Article 6 (4) GDPR.
[19] See preamble 50 GDPR.

the possibility that the new legal basis of the other controller may be based on the same section in Article 6 (1) GDPR as the legal basis of the controller who collected the personal data.

Note: The provision of personal data by the insolvency practitioner to another controller, for example, in the context of realisation of the estate, cannot take place on the basis of compatibility with the collection purposes. If an insolvency practitioner, in its capacity as controller, intends to provide personal data to another controller in this context, the prior consent of the data subject(s) is generally required in accordance with Article 7 GDPR.[20] This other controller must be able to base the processing of the personal data on its own legal basis within the meaning of Article 6(1), GDPR, such as consent from or an agreement with the data subject within the meaning of Article 6(1)(a) or (b), GDPR.

Fairness
Fair processing of personal data means, among other things, that personal data must be adequately secured, which means that appropriate technical and organisational measures have been taken to guarantee the availability, integrity and confidentiality of the personal data. This may also mean that the insolvency practitioner will have to take measures to ensure that the personal data present in the estate are not processed unlawfully, even after the settlement of a liquidation (see, among others, Scenarios IV and V in the remainder of this letter).

Transparency
In short, the transparency obligation means that the controller takes appropriate measures to provide data subjects with information regarding the (intended further) processing of their personal data and the rights they can rely on vis-à-vis the controller.[21] In this way, data subjects are enabled to exercise their (GDPR) rights towards the controller.[22] A controller must facilitate the exercise of these rights in an adequate manner. If there is intended further processing for other purposes, the insolvency practitioner must properly inform the data subjects in advance.[23]

Accountability
Controllers are accountable, which means that the insolvency practitioner, in that capacity, must be able to demonstrate that the aforementioned and other data processing principles set out in Article 5 GDPR have been complied with.[24]
This means, among other things, that the insolvency practitioner must document the relevant facts and circumstances, considerations, conclusions and the final assessment with regard to the compatibility test.

Nature of personal data and DPIA obligation

[20] Cf. Scenario II. Scenario II deals with contract takeover, in which context, to the extent necessary, personal data are processed for the performance of a contract with the data subject.
[21] See Article 12 GDPR. See also the EDPB guidelines on the transparency obligation: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp260rev01_nl.pdf.
[22] See Article 15 et seq. GDPR.
[23] See Article 13 (3) GDPR.
[24] Other principles include 'data minimisation', 'accuracy', 'storage limitation' and 'integrity and confidentiality'. See Article 5 GDPR.

Furthermore, it is important to emphasise that the nature (sensitivity) of the personal data may entail additional conditions and obligations, such as in the case of special categories of personal data, personal data regarding criminal convictions and criminal offences and the citizen service number (Dutch: BSN).

Insolvency practitioners must consider the risks to the rights and freedoms of data subjects associated with processing. The risks for data subjects associated with processing personal data partly determine the lawfulness or unlawfulness of processing and the manner in which controllers must fulfil their obligations. The more sensitive the personal data (whether or not due to the context in which they are processed), the higher the processing-related risks for the rights and freedoms of the data subjects, and the more carefully these data must be handled.

If a new or changed processing operation - taking into account its nature, scope, context and purposes - is likely to result in a high risk for the rights and freedoms of natural persons, the controller must carry out a so-called data protection impact assessment (abbreviated to 'DPIA').[25]

This means that, prior to processing, it is assessed what effect the intended processing activities have on the protection of personal data, and, where necessary, measures are taken to mitigate risks. For certain processing operations, carrying out a DPIA is, in any case, mandatory.[26] If the DPIA shows that the processing would pose a high risk and the controller cannot take further measures to mitigate these risks, the controller must consult the Dutch Data Protection Authority (DPA) prior to processing.[27]

Administration and liquidation of the estate of a company in liquidation

Under the Bankruptcy Act, the insolvency practitioner is charged with the administration and liquidation of the estate of a company in liquidation. When administering and liquidating an estate of a company in liquidation, an insolvency practitioner must continuously consider whether personal data are processed in the associated activities. If the answer is affirmative, it must be assessed whether the relevant (intended) processing operations can be based on a legal basis within the meaning of Article 6 GDPR , and - more generally - whether this is done in accordance with the GDPR. The Dutch Data Protection Authority (DPA) emphatically points out the insolvency practitioner's own responsibility.

Scenario descriptions

The following are a number of relevant scenarios (non-exhaustive list) in which an insolvency practitioner should be alert to the applicable data protection rules:

- Scenario I: Continuation of (a part of) the insolvent legal entity by the insolvency practitioner;
- Scenario II: Takeover of the existing legal relationship of an insolvent legal entity with its customers;
- Scenario III: Sale of personal data;
- Scenario IV: Monetisation of assets, in the course of which personal data may be processed; and

[25] See Article 35 GDPR.
[26] See: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667.
[27] See Article 36 GDPR.

- Scenario V: The insolvent legal entity ceases to exist.

The points of attention relevant to the previous scenarios from a data protection perspective are further elaborated below. It is important for the insolvency practitioner, among other things, to determine whether the insolvency practitioner is providing personal data to another (acquiring) controller or not.

These scenarios assume lawful initial processing of personal data. Scenario I: Continuation of (the activities of) the same insolvent legal entity by the insolvency practitioner

In cases of a (temporary) continuation of (the activities of) the same insolvent legal entity, the same legal entity, whether or not in a changed form, is in fact continued by the insolvency practitioner with the aim of realising a going-concern sale of the insolvent legal entity.

The continuation of the insolvent legal entity is based on the situation where, in the context of continued activities, personal data will in fact be processed by the same controller for the same purposes as the original processing purposes prior to the liquidation. So in fact, the controller and the processing purposes do not change.

If in such cases nothing (material) changes for the data subjects from a data protection perspective, the processing of the personal data already legally processed can in principle continue to take place based on the original legal basis or bases. Naturally, data subjects involved in the continuation of (a part of) an insolvent legal entity must be properly informed about the associated consequences for their personal data.

However, different rules apply if processing does not involve the continued processing of personal data in bankruptcy by the same controller, for example in the event of further processing by the same controller for purposes other than the purposes for which the personal data were collected.

Further processing of personal data by the same controller
It may be the case that during liquidation, there is a wish to further process personal data in the estate of the insolvent legal entity, for purposes other than the purposes for which the personal data were initially collected. Such further processing of personal data is only permitted if:
(i) the data subjects have given consent for this in accordance with Article 7 GDPR;
(ii) there is an applicable specific legal authority or a specific statutory obligation to do so as referred to in Article 6(4) GDPR; or
(iii) it concerns compatible further processing.

All relevant facts and circumstances of the case must be taken into account in the compatibility assessment. If the controller concludes on the basis of Article 6(4) GDPR that the processing operation is

compatible, the further processing of the personal data can in principle be based on the original legal basis for collection.[28]

Scenario II: Takeover of the existing legal relationship of an insolvent legal entity with its customers
The existing legal relationships of the insolvent legal entity with its customers can be taken over by another legal entity or natural person ('contract takeover'[29]).

If the contract takeover takes place lawfully, in compliance with all applicable rules, the personal data necessary for the contract takeover can be transferred to the new contracting party.

A significant aspect in this case is whether, in the event of a contract takeover, the data subject[30] has, in the context of the cooperation requirement, indeed been informed and been given the opportunity to agree or object to (parts of) the contract takeover and therefore against the necessary provision of his personal data.

In this context, this concerns the personal data that are necessary for the performance of the contract. In such cases, the insolvency practitioner can provide the personal data in question to the new contracting party on the basis of Article 6(1)(b) GDPR.

It goes without saying that the new contracting party must process the personal data, as a controller, in accordance with the GDPR. This means, among other things, that if there are special categories of personal data or personal data about criminal convictions and criminal offences, on the side of the controller - in addition to a legal basis within the meaning of Article 6 (1) GDPR – explicit consent of the data subject or another legally valid exception is required in order to process the personal data in question.[31]
With regard to the citizen service number, this identification number may only be processed if and to the extent necessary for the implementation of purposes determined by law.[32]

Scenario III: Sale of personal data
When selling personal data (e.g. in the form of a customer database) - without them forming part of a contract takeover, after which the new contracting party will continue the existing legal relationship of the insolvent legal entity with the data subjects - it constitutes a provision to another controller.
Such provision does not constitute compatible processing within the meaning of Article 6(4) GDPR. Such provision of personal data must be based on the prior consent of the data subject(s) in accordance with Article 7 GDPR.

Scenario IV: Monetisation of assets, in the course of which personal data may be processed

[28] The foregoing is without prejudice to other potentially applicable rights and contractual or statutory obligations. With regard to health data, applicable provisions of the Medical Treatment Contracts Act may be considered.
[29] See Article 6:159 Dutch Civil Code
[30] See Article 6:159 Dutch Civil Code.
[31] See Articles 9 and 10 GDPR and Articles 22 et seq. and 31-33 UAVG.
[32] See Article 87 GDPR and Article 46 UAVG.

If, for example, an insolvency practitioner wishes to monetise equipment, including digital data carriers (e.g. in computers or laptops), the insolvency practitioner must ensure that the equipment does not or no longer contains any data carriers or that the personal data on the relevant data carriers are irreversibly destroyed before the equipment is disposed of.[33] It may be wise to call in specialists for this, in accordance with the GDPR[34] .

Scenario V: The insolvent legal entity ceases to exist

Lastly, an insolvent legal entity can cease to exist through dissolution.[35] This is, among other things, the case at the time when the liquidation ends. The insolvency practitioner reports the termination of the liquidation to the registers where the insolvent legal entity is registered.[36]

The estate may still contain personal data (e.g. the customer file) at the time of termination of the liquidation (dissolution). After a legal entity has ceased to exist due to dissolution, it will be necessary to determine what personal data have remained in the estate, what should be done with those personal data and who is responsible for those personal data in that context.

In general, the controller must ensure that all personal data are irreversibly destroyed if the processing of the personal data is no longer necessary for the purposes for which they were collected and further processed.[37] If a legal entity has ceased to exist, personal data will in general no longer be necessary for the purposes for which they were collected and further processed.

However, a statutory retention period may apply to certain personal data, for example, a retention period in healthcare legislation, in tax legislation or the Public Records Act. In that case, the controller must, among other things, ensure that the personal data in question are retained for the applicable retention period, are adequately secured and, after the applicable retention period(s), are destroyed after all. The controller must ensure that data subjects can exercise their GDPR rights during that retention period.

It follows from the Bankruptcy Act that the books and papers found in the estate by the insolvency practitioner are handed over to the debtor.[38] This usually means that books, documents and other data carriers - after the legal entity has ceased to exist – are retained by the custodian within the meaning of Article 2:24 of the Dutch Civil Code. This custodian must be included as such in the registers in which the dissolved legal entity was entered.[39] In those cases, the custodian is the controller and, as such responsible for the personal data retained by him or on his behalf.

[33] This is without prejudice to other obligations relating to the personal data concerned (e.g. retention obligations and the principle of data minimisation).
[34] This may include the obligation to enter into a processing agreement if a processor within the meaning of Article 4 (8) GDPR is engaged.
[35] See Article 2:19 Dutch Civil Code
[36] See Article 2:19 (6) Dutch Civil Code.
[37] It may be advisable to call in specialists when destroying personal data.
[38] See Article 193 (3) Bankruptcy Act.
[39] See Article 2:24 (3) Dutch Civil Code.

If there is no custodian and no custodian is appointed by the court, the insolvency practitioner - as the final controller - will, with regard to the personal data in the books, documents and other data carriers, have to ensure compliance with the GDPR, UAVG and other applicable laws and regulations.

If the books, documents and other data carriers in the custody of the custodian or the insolvency practitioner contain special categories of personal data or personal data about criminal convictions and criminal offences, on the side of the controller - in addition to a legal basis within the meaning of Article 6 (1) GDPR – explicit consent of the data subject or another legally valid exception is required in order to process the personal data in question.

With regard to the citizen service number, this identification number may only be processed if and to the extent prescribed by law and the processing is necessary for the implementation of purposes determined by law.[40]

Conclusion
The Dutch Data Protection Authority (DPA) intends to invite you for a consultation in the near future. Please be reminded that this letter does not detract from the authority of the Dutch Data Protection Authority (DPA) to investigate possible violations (ex officio).

A copy of this letter has been sent to the General Council of the Netherlands Bar. The Dutch Data Protection Authority (DPA) also intends to post the contents of this letter on its website.

Kind regards,
On behalf of the Dutch Data Protection Authority (DPA),

Ir. C.M. Schut, MPA
Director of System Supervision, Security and Technology

[40] See Article 46 UAVG.