



LEMVERIFY

# ACHIEVING GDPR DATA MINIMISATION COMPLIANCE

BEST PRACTICE OVERVIEW: DATA REDACTION

WHITE PAPER

## Summary

This paper examines the **data minimisation** principle of the GDPR. It looks at what minimisation means and why it matters to data controllers and data processors.

Specifically, it explains how GDPR compliance can be achieved through the **redaction of unnecessary data**.

Redaction is the process of blocking extraneous data by either removing it or replacing it with a permanent and uneditable box to mask the underlying material.

LEM Verify offers a redaction service to help companies develop best practice in their processing of personal data. Two methods are available from LEM Verify:



### Automatic redaction

Client documents are redacted instantly during the authentication process. This is offered as part of the standard LEM Verify document verification process to all clients.



### Redaction processing at scale

Retroactive processing of existing scans of identity documents. Large quantities can be batch processed through an API to ensure existing records are fully compliant, and to reduce security risk.

LEM Verify is a UK-based RegTech specialising in identity verification. As well as confirming the authenticity of identity documents, LEM Verify offers a facial biometric service to match customers to their documents.

LEM Verify delivers automated compliance with no complex IT integration, and low-cost pay as you go pricing.

## What is data redaction?

Redaction is the process of removing unnecessary data. It is a permanent action, whereby extraneous data is hidden. It's the equivalent of using a pen to black out text on a photocopy, or physically cutting out text like a censor.


LEM Verify redacts data by editing the original scan, embedding black blocks on unnecessary data fields so only required data is shown.



*The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.*



## Data Minimisation




### PASSPORT VERIFICATION REPORT

✕ REFER

**REFER REASON**  
Specimen document

**DOCUMENT TYPE**  
Passport



#### Personal Information

**TITLE**

**GIVEN NAMES**  
ANGELA ZOE

**SURNAME**  
UK SPECIMEN

**GENDER**  
FEMALE

**NATIONALITY**  
BRITISH CITIZEN

**BIRTHPLACE**  
CROYDON

**DOB**  
04/12/1988

#### Document Information


**DOCUMENT NUMBER**  
\*REDACTED\*

**ISSUING COUNTRY**  
\*REDACTED\*

**EXPIRY DATE**  
28/09/2025

**ISSUE DATE**  
28/09/2015

**ISSUING ORGANISATION**  
\*REDACTED\*

**COUNTRY**  


**MRZ LINE 1**  
\*REDACTED\*

**MRZ LINE 2**  
\*REDACTED\*

#### Analysis

ALL INFORMATION CAPTURED

FACE CAPTURED


SUSPICIOUS DATA

NOT EXPIRED

**PART OF COMBINATION**  
pEP2B9xpSZgKCHXNAMTw2Q

**PREPARED FOR**  
paul+test2@lemdata.com

**ACCOUNT**  
d02f21af-06c9-4c06-adaa-b636746c4c03



POWERED BY LEM VERIFY

The GDPR **lists seven key principles** for data protection. Companies have spent years ensuring compliance with these principles, primarily focussing on the consent and processing provisions.

The issue of **minimisation** has not received the same amount of high-level coverage, but as a key principle it must be addressed. Article 5 (1) (c) states:

**Personal data shall be:**

**(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')**

**As explained by the Information Commissioner's Office (ICO):**

Firms must ensure the personal data they are processing is:



#### **Adequate**

sufficient to properly fulfil your stated purpose.



#### **Relevant**

has a rational link to that purpose.



#### **Limited to what is necessary**

you do not hold more than you need for that purpose.



#### **The ICO checklist is straightforward:**

- We only collect personal data we actually need for our specified purposes.
- We have sufficient personal data to properly fulfil those purposes.
- We periodically review the data we hold, and delete anything we don't need.

## Risks & Challenges

In practical terms, when collecting and storing customer documents for KYC and AML purposes, this means:

- only gathering the information needed
- redacting any part(s) of the data that are not necessary

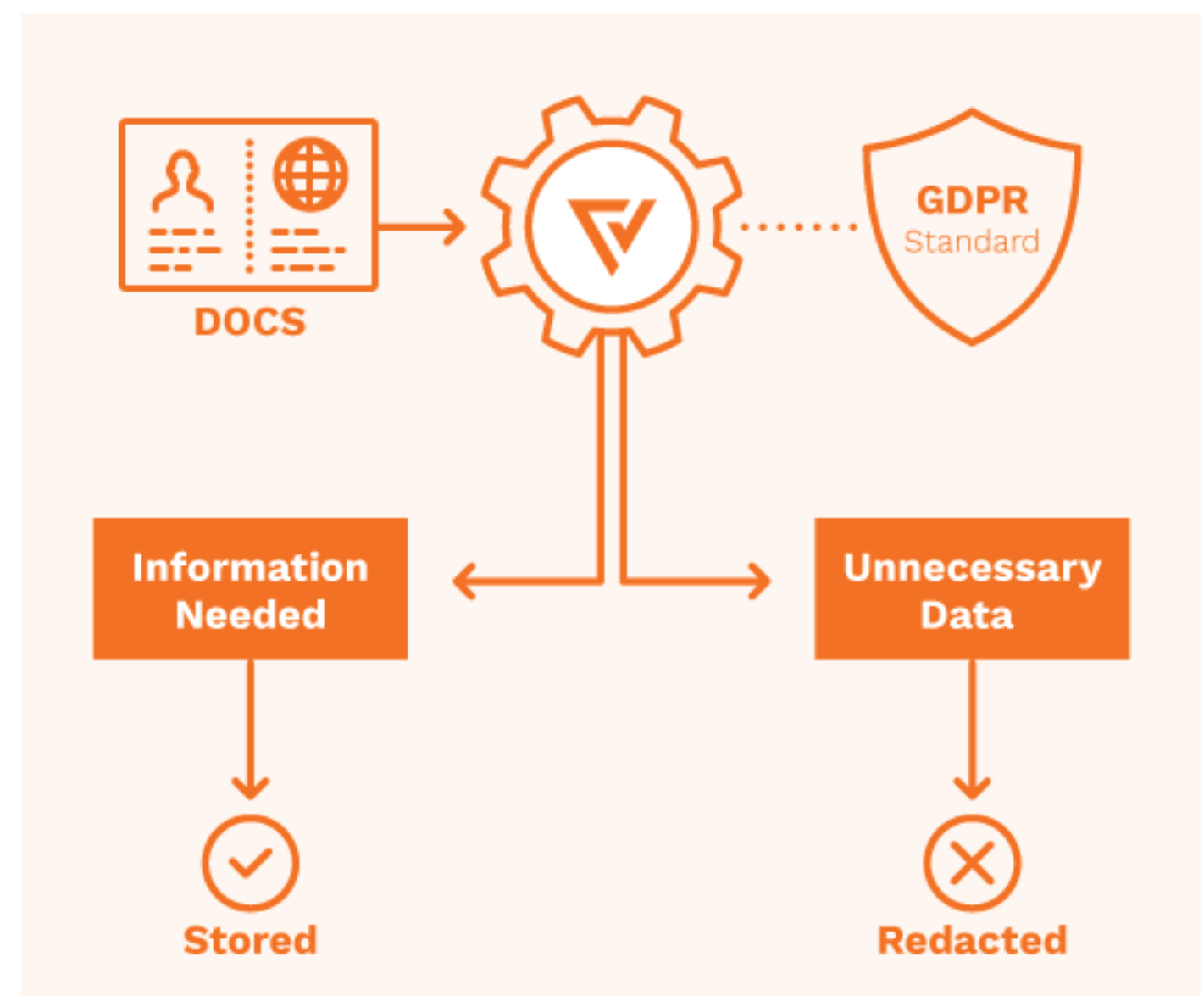
When a company saves a copy of a customer's document, there is a good chance that additional and irrelevant data will be saved. Admittedly this is by chance rather than by design, but nonetheless it exposes the firm to potential sanctions if this additional data is found not to meet the minimisation requirement. There has been a historic impulse to save all data indefinitely – just in case – but this is no longer appropriate.

### Example:

A professional service firm needs to verify and store client identification documents as part of regular KYC/AML checks. Full copies of passports and driving licences are retained. However, elements of the data (such as document number, valid dates, issuing organisation etc) are irrelevant for these purposes, once the document has been verified. To make sure the stored data is adequate, relevant and limited to what is necessary, the extra fields should be redacted.

As well as this **compliance risk**, there is potential **reputational risk** to mitigate. If a company suffers a data breach and client documents are shared publicly, the company will be criticised and censured for the impact this could have on individuals affected.

There is however, a significant and practical challenge to ensuring compliance. **Current systems and processes may not have the ability to redact data**, meaning that many firms are storing more personal identification information than they need, and risk fines for non-compliance.



## GDPR Fines/Penalties

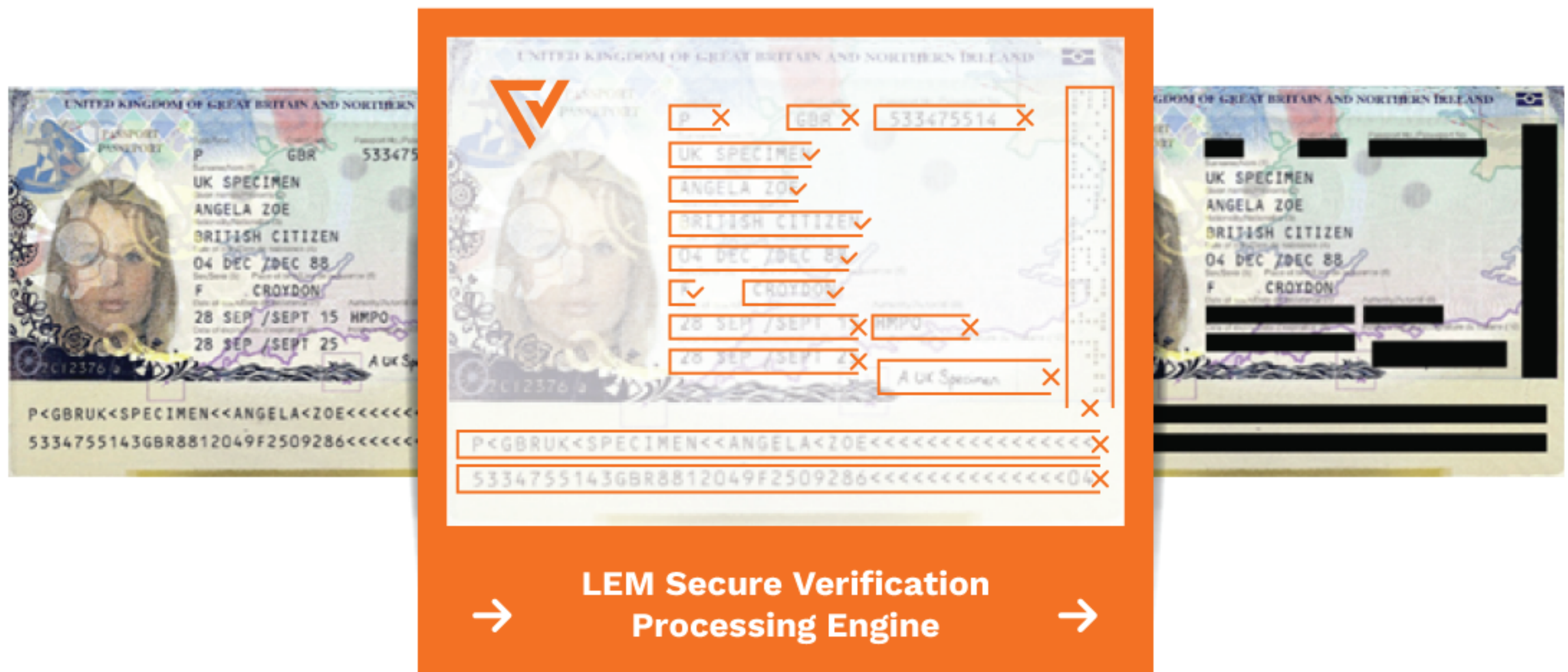
Article 83 of the GDPR details the monetary penalties which can be applied for failure to comply. The Higher Maximum amount of EUR 20 million (or local currency equivalent) or 4% of total annual worldwide turnover in the preceding financial year, whichever is higher. The Standard Maximum applies to less severe infringements and is set at EUR 10 million (or local currency equivalent) or 2% of total annual worldwide turnover in the preceding financial year, whichever is higher.

## Redaction: the LEM Verify solution

LEM Verify is a UK-based RegTech specialising in identity verification. As well as confirming the authenticity of identity documents, the machine learning algorithm uses the video camera on smart devices to match faces with documents and deter fraud.

Copies of customer identity documents are automatically processed and supplied to data controllers.

To ensure compliance full compliance with the data minimisation principle, LEM Verify can redact unnecessary data while processing identity documents at scale.



This service is flexible and customisable, as LEM Verify recognises that different firms and industries have different data collection requirements. Companies can specify the data points they need to save to meet regulatory needs and maintain GDPR compliance.

## Redaction vs Pseudonymisation - what's the difference?

Redaction is the process of removing unnecessary data. It's a permanent action, where extra data is hidden.

### Is redaction the same as pseudonymisation?

The processes are related but not the same. Pseudonymisation is masking personal data in such a way that it can no longer be attributed to a specific data subject, without the use of additional information. Using a "pseudonym key" allows data processors to reveal the original data. Redaction is a permanent measure; once the source image has been redacted, there is no way to retrieve the original data that has been hidden.

**LEM Verify redacts data by editing the original scan**, embedding black blocks on unnecessary data fields so only necessary data is shown - it does not allow pseudonymisation.

## Instant redaction of uploaded documents:

For clients using LEM Verify for instant verification:



## Automated redaction at scale:

Batches of existing document scans are processed together:



If needed, the LEM Verify process will also crop and de-skew the document images for ease of future use.



LEM Verify's redaction service offers many benefits:

- Best practice compliance with GDPR rules on data minimisation.
- Automated process – no manual intervention at any stage.
- Reduce compliance, security and reputational risks.

The redaction feature is available to all LEM Verify accounts and is easily set up from the client dashboard. Please contact [sales@lemverify.com](mailto:sales@lemverify.com) for further details or try it out for yourself.



# LEMVERIFY

For more information about LEM Verify,  
please contact [sales@lemverify.com](mailto:sales@lemverify.com)

Disclaimer:

The document authentication and redaction features in LEM Verify requires you provide a good quality image in order to be able to authenticate and redact an identity document. End users are responsible for ensuring the quality of the image provided, and LEM Verify takes no responsibility for the image quality. LEM Verify and the LEM Verify logo are registered trademarks of Less Equals More Ltd. Other products and services may be trademarks or registered trademarks of their respective companies. No part of this document may be reproduced without the express permission of LEM Verify. Less Equals More Ltd, operating under the trading name of LEM Verify is a company registered in England & Wales at 37 Meadowlands, West Clendon, Guildford, United Kingdom, GU4 7TA. Registration number 10546666.