

Dateneigentümer (Data Owner)

Ein Auszug aus dem [SOP-Download 400-01 Datenintegrität und Data Governance](#)



von Dr. Christine Oechslein



Der Begriff der **Dateneigentümerschaft** ist in vielen Pharmaunternehmen noch nicht klar definiert. Auch sind die entsprechenden Verantwortlichkeiten oft nicht eindeutig und lückenlos geregelt. Als Voraussetzung für ein funktionierendes und GxP-konformes Datenmanagement muss jedoch firmenspezifisch verständlich geregelt und geschult sein, wer jeweils „Prozesseigner“/Process Owner ist, wer „Dateneigentümer“/Data Owner ist und wie andere Benutzerrollen oder Funktionen davon abgegrenzt sind.

Für die Festlegung der Dateneigentümerschaft gibt es noch keine regulatorischen Vorgaben. Daher sind unterschiedliche Lösungen möglich, die je nach betrieblicher Organisation Vor- oder Nachteile haben: Grundsätzlich sollten jedoch Daten, die innerhalb einer Abteilung/ eines Bereichs generiert wurden, über die gesamte aktive Phase des Datenlebenszyklus in deren Eigentümerschaft verbleiben. Beim Übergang zur inaktiven Phase, also bei der Übergabe an ein Archiv, gibt es mehrere Möglichkeiten, z. B.:

- Wird das Archiv von der datenerzeugenden Abteilung selbst organisiert und verantwortlich geführt, ist es sinnvoll und praktikabel, dass die Daten in der ursprünglichen Eigentümerschaft verbleiben.
- Bei Datenübergabe an größere, ggf. zentrale und/oder räumlich entfernte Archive kann es zur Datensicherheit beitragen und Ressourcen schonen, wenn die Daten-Eigentümerschaft z. B. an eine zentrale Q-Funktion übergeben wird. Vorteil: Über die ausgedehnten Zeiträume der Archivierung gibt es zahlreiche Personalwechsel in den Linienfunktionen. Jedes Mal müssten die nachfolgenden Dateneigner dem Archivverantwortlichen gemeldet werden – und die neuen Dateneigner aus der Linie müssten für uralte Datensätze Verantwortung tragen, die lange vor ihrer Zeit entstanden sind. Die vielen Schnittstellen dieser Konstellation bergen Risiken bzgl. der Kontinuität, weshalb eine Eigentumsübergabe an eine zentrale Funktion vorteilhaft sein kann.

Dateneigentümer (Data Owner) sind Personen mit einer Funktion im mittleren Management, welche die Verantwortung für die zu ihren Geschäftsprozessen gehörigen Daten und Dokumenten tragen.

Werden Daten mehrfach weitergegeben, z. B. zur Auswertung oder Archivierung in andere Systeme übertragen, von Dienstleistern übergeben oder von Datenspeichern (Speichermedien, Backup-Systeme) eingelesen, dann erfordern diese zahlreichen Schnittstellen ganz besondere Aufmerksamkeit, die nur ein Mitarbeiter mit ausreichendem fachlichen Überblick und gleichzeitiger Leitungsfunktion übernehmen kann.

Somit ist der Dateneigentümer in der Regel gleichzeitig Geschäftsprozesseigner (Business Process Owner, BPO – meist der Leiter des jeweiligen Bereiches). Er ist dafür verantwortlich, dass

sämtliche GxP-Daten seiner Geschäftsprozesse sowohl in der aktiven als auch in der inaktiven Phase des Daten-Lebenszyklus „integer“ bleiben.

Die abstrakten Begriffe „**Dateneigentümer**“ und „**Geschäftsprozesseigentümer**“ (**BPO**) sind keine Begriffe aus der GMP-Welt. Sie lassen sich auch nicht direkt den GMP-Verantwortungsträgern „Leitung der Herstellung“, „Leitung der Qualitätskontrolle“ und „Sachkundige Person“ zuordnen. Daher ist eine wichtige Voraussetzung für das Datenmanagement, dass jede Firma selbst definiert:

1) *Welche Geschäftsprozesse gibt es im Unternehmen? Wer ist der jeweilige BPO?*

Beispiele: Geschäftsprozess „Produktion Feste Formen“ – Leiter Herstellung Feste Formen; Geschäftsprozess „Gebäude und Betriebsmanagement“ – Leiter Technik; Geschäftsprozess „Rohstoffbeschaffung“ – QA-Verantwortlicher für Rohstoffqualität (als koordinierende Funktion zwischen Einkauf, Rechtsabteilung und Labor)

2) *Welche GxP-relevanten Daten entstehen im Zusammenhang mit dem Geschäftsprozess?*

Es ist sinnvoll, den BPO auch zum Eigentümer der zugehörigen Daten (**Data Owner**) zu machen, da er den nötigen Überblick hat, um weitreichende Entscheidungen zu fällen, z. B. wenn bestimmte Teilbereiche samt Daten an andere Standorte übergeben werden, eine Umstellung von manueller auf elektronische Datenerfassung geplant oder Digitalisierung bestimmter Datenpakete erwogen wird. Ein „**Dateneigentümer**“ sollte einerseits noch genügend Einblick in die Arbeitsabläufe vor Ort haben, um Gefahren für Daten und Dokumente einschätzen zu können, die in den verschiedenen Arbeitsbereichen generiert werden. Andererseits benötigt der Dateneigentümer ausreichende Managementbefugnisse und Überblick, um zusammengehörige Datenpakete sinnvoll zu strukturieren und ihrem Verlustrisiko entsprechend zu sichern.

3) *Welche Unterprozesse gibt es zu jedem Geschäftsprozess? Wer sind die zugehörigen Process Owner?*

Geschäftsprozesse bestehen oftmals aus unterschiedlichen Teil- oder Subprozessen, die organisatorisch in verschiedenen Verantwortungsbereichen angesiedelt sein können. So gehören beispielsweise zum Geschäftsprozess „Rohstoffbeschaffung“ Teilprozesse im Einkauf, in der Rechtsabteilung, in der QS, am Lager, in der QK usw. Die Prozesseigner dieser Teilprozesse sind zumeist sinnvollerweise auch für den Umgang mit den entstehenden Daten verantwortlich zu benennen – als „**Responsible User**“ (RU). Der Verantwortliche User (RU) verwaltet und kontrolliert die von Usern generierten Daten und bereitet sie nach Abschluss der aktiven Phase zur Archivierung vor.

4) *Welche User gehören zum jeweiligen Prozess?*

Die Gruppe der **User** ist zumeist nicht homogen: hier muss festgelegt sein, wer tatsächlich **Datenerzeuger** ist, wer (außer dem RU) kontrollieren und/oder auswerten darf und wer nur Leseberechtigung hat.

Hinweis: Je nach Organisation eines Unternehmens können „Dateneigentümer“ auch auf niedrigeren Hierarchiestufen definiert werden – zusammen mit den damit verbundenen Pflichten im Umgang mit den Daten. Wenig empfehlenswert ist es jedoch, jeden „Erzeuger“ von Daten (z. B. Produktionsmitarbeiter, Labormitarbeiter) zum „Dateneigentümer“ zu ernennen.

Sehr sorgfältig zu regeln sind die Schnittstellen/Besitzübergänge, wenn Datenpakete an andere Dateneigentümer übergeben werden, z. B. bei Ausscheiden eines Mitarbeiters oder Ausgliederung von Geschäftsbereichen. Wenn es *vielen* Data Owner auf *einer* unteren Hierarchiestufe gibt, dann ist aufgrund der normalen Mitarbeiter-Fluktuation die Anzahl der sauber zu regelnden Daten-Besitzübergänge sehr hoch. Dateneigentümer in höheren Hierarchiestufen (unteres/mittleres Management) sind zwar für größere Datenpakete

verantwortlich aber hier sind Nachfolgeregelungen und Übergaben von Aufgaben und Verantwortlichkeiten im Interesse der Firma in der Regel deutlich besser strukturiert – eine Voraussetzung für Datensicherheit.

Jeder Dateneigentümer ist dafür verantwortlich, schriftlich (in Form von Arbeitsanweisungen bzw. bei externen Partnern in Form von Verträgen) genau zu regeln

- wie die Aufgaben und Verantwortlichkeiten zwischen ihm und den Responsible Usern in seinem Bereich aufgeteilt sind
- wie die Schnittstellen/Besitzübergänge definiert sind, wenn er Datenpakete von anderen Dateneigentümern übernimmt oder an andere Dateneigentümer übergibt, z. B. bei Verlagerung/Ausgliederung von Prozessen oder Geschäftsbereichen, bei Ausscheiden von Mitarbeitern, aber auch Vertreter- & Nachfolgeregelung für die eigene Person
- wie die Aufgaben, Verantwortlichkeiten und Kommunikationswege zwischen ihm und außerhalb seines Verantwortungsbereiches befindlichen Archiven verteilt sind, z. B. Archive in anderen Abteilungen oder bei externen, qualifizierten Auftragnehmern.

Quelle:

Dieser Text ist ein Auszug aus dem [SOP-Download 400-01 Datenintegrität und Data Governance](#)



Ziel dieser SOP ist es, einen Überblick zu geben, welche Strategien, Maßnahmen und Abläufe etabliert sein müssen, um stets die Herrschaft über GxP-relevante Daten zu haben (Data Governance) und somit ihre Integrität über den gesamten Daten-Lebenszyklus sicherzustellen. Das bezieht sich sowohl auf herkömmliche Papier-Dokumente, als auch auf Daten aus IT- Systemen.

Diese SOP legt fest,

- wie ein Daten-Lebenszyklus definiert ist,
- wer in Ihrem Unternehmen "Dateneigentümer" ist und wofür er verantwortlich ist,
- wie die "ALCOA plus"-Anforderungen grundsätzlich zu verstehen und anzuwenden sind,
- in welchen SOPs die einzelnen Detailregelungen und Verantwortlichkeiten festgelegt sind, die eine gesetzeskonforme Datenintegrität gewährleisten.

Jetzt bestellen:

<https://www.gmp-verlag.de/de/datenintegritaet/sop-datenintegritaet.html>

Autorin:

Dr. Christine Oechslein

Apothekerin

GMP-Praxis, Bad Säckingen

E-Mail: c.oechslein@gmp-praxis.de