Gesamtbetriebsvereinbarung

zur Durchführung der Prüfungen
von Corporate Auditing mittels digitaler Datenanalysen

Präambel

Die interne Revision ist eine unabhängige Funktion, die weltweit innerhalb des Konzerns Strukturen, Prozesse und Aktivitäten prüft und beurteilt. Sie ist ein integraler Bestandteil der Corporate Governance der Bayer-Organisation. Der Auftrag der internen Revision umfasst u. a. die

- Kontrolle der Einhaltung von Gesetzen und internen Regelungen,
- Sicherstellung der Wirksamkeit des internen Kontrollsystems,
- Verhinderung von Vermögensverlusten und die
- Unterstützung des Vorstandes bei der Wahrnehmung der Sorgfaltspflichten.

Zu den Aufgaben der internen Revision gehören die Prüfung und Beurteilung

- der Effizienz und der Effektivität des internen Kontrollsystems,
- der ordnungsmäßigen Rechnungslegung,
- der Qualität, mit der die jeweiligen Prozesse im Aufgabenbereich beachtet und erfüllt werden,
- des Handelns der Funktionsträger bezüglich der Einhaltung relevanter gesetzlicher und interner Vorschriften,
- inwieweit die Vermögensgegenstände des Unternehmens geschützt sind und diese wirtschaftlich eingesetzt und genutzt werden, sowie
- von fallbezogenen Einzelprüfungen, insbesondere bei Verdacht einer Unternehmensschädigung.

Aufgrund der Zunahme datenverarbeitungsgestützter Abläufe im Unternehmen werden die Prüfungsmethoden von Corporate Auditing fortlaufend angepasst und zeitgemäß durch computergestützte Prüfungsverfahren verstärkt. Dies ersetzt aber nicht die nach wie vor erforderlichen klassischen Prüfungshandlungen – Fallprüfungen anhand von Unterlagen – sondern unterstützt lediglich die gezielte Auswahl der Vorgänge, die aufgrund eines vorgegebenen Prüfungsziels als relevant anzusehen sind.

(Die vorangegangene Beschreibung der Aufgaben der internen Revision hat nicht zum Ziel, diese der Mitbestimmung zu unterwerfen)

1. Geltungsbereich

Diese Gesamtbetriebsvereinbarung wird abgeschlossen für alle Beschäftigten der Bayer AG sowie kraft Vollmacht der mit der Bayer AG verbundenen Konzernunternehmen Bayer CropScience AG, Bayer MaterialScience AG, Bayer HealthCare AG, Bayer Pharma AG, Bayer Animal Health GmbH, Bayer Business Services GmbH, Bayer Technology Services GmbH, Bayer Direct Services GmbH, Bayer Intellectual Property, der Bayer MaterialScience Energiegesellschaft Brunsbüttel und Pallas AG (alle Gesellschaften nachstehend „GESELLSCHAFTEN" genannt).

Sie gilt nicht für Leitende Angestellte i.S.d. § 5 Abs. 3 BetrVG der GESELLSCHAFTEN.

2. Prüfungsplanung

Im Rahmen der Planung einer risikoorientierten Prüfung erfolgt durch die interne Revision eine frühzeitige Festlegung der Prüfungsthemen nach Arbeitsgebieten und Gesellschaften. Sie wird mit dem Vorstand abgestimmt und genehmigt und dem Prüfungsausschuss des Aufsichtsrates der Bayer AG vorgestellt. Im laufenden Jahr können Ergänzungen und Anpassungen zu dieser Planung erfolgen, z. B. aufgrund von aktuellen Erkenntnissen, Beauftragungen der Entscheidungsträger oder Meldungen/Anträgen der Compliance- Organisation.

3. Digitale Datenanalyse

Die digitale Datenanalyse basiert grundsätzlich auf der Gesamtheit der herunter geladenen Rechnungswesendaten und trägt - neben der Vermeidung einer subjektiven Datenauswahl - insbesondere zur Neutralität und Objektivierung des Prüfens bei. Dies erfolgt durch die Umsetzung der sachbezogenen Kriterien und Fragestellungen in standardisierten Auswertungs- und Analyseschritten, mit denen die Ursprungsdatenmenge auf die Einhaltung gesetzlicher Vorschriften und interner Regelungen analysiert werden kann. Identifikationsdaten von Mitarbeitern werden dabei nicht als Auswertungskriterium verwendet. Durch die nacheinander erfolgenden Analyseschritte wird die Datenmenge auf das Maß reduziert, welches anschließend auf konventionelle Weise durch das zuständige Prüfungsteam von Corporate Auditing bearbeitet wird.

Die digitale Datenanalyse vollzieht sich in sechs Schritten, die sämtlich dokumentiert und protokolliert werden:

I. Datenanforderung
Eine Datenanforderung erfolgt ca. 6-8 Wochen vor einer Prüfung und wird durch einen Prüfungsleiter initiiert. Datendownloads erfolgen grundsätzlich nur prüfungsbezogen und werden dokumentiert.

II. Datendownload
Der Datendownload kann nur von einem eng definierten Personenkreis durchgeführt werden. Hierbei werden personenbezogene Daten pseudonymisiert heruntergeladen. Zur Pseudonymisierung und Entschlüsselung ist ein Passwort nötig. Sollte eine Pseudonymisierung aufgrund eines konkreten Verdachtfalles aufgehoben werden müssen, so erfolgt dies ausschließlich auf Anforderung des Prüfungsleiters, hierbei wird gemäß Ziffer 2 verfahren.

III. Qualitätssicherung
Um Vollständigkeit und Plausibilität der Daten sicherzustellen, werden die Daten statistisch und inhaltlich validiert. Unter statistischer Validierung wird die Überprüfung der Vollständigkeit der Datensätze verstanden; im Zuge der inhaltlichen Validierung werden die Daten, soweit möglich, einer kaufmännischen Plausibilisierung unterzogen.

IV. Datenübergabe
Die Datenübergabe an die Revisoren erfolgt auf verschlüsselten Datenträgern. Im Zuge der Übergabe unterzeichnet der Revisor eine Verpflichtungserklärung, die die Einhaltung von Gesetzen und Richtlinien beinhaltet (siehe Anlage 1).

V. Prüfung
In der Phase der Prüfung werden die Daten durch die Revisoren mit logischen Abfragen manuell oder automatisch analysiert. Diese Klassifizierung findet ausschließlich risikoorientiert nach revisionsrelevanten Vorgängen statt.

VI. Datenlöschung
Nach der Prüfung werden die Daten gelöscht und nur berichtsrelevante Informationen archiviert.

Ziel der Analyse ist nicht die Leistungs- und Verhaltenskontrolle einzelner Mitarbeiter. „Mitarbeiter-Screenings", ein Gegenlaufen von Daten (so genanntes Matching) oder Datenabgleiche aller Mitarbeiter/innen oder von Mitarbeitergruppen finden nicht statt und auch in den Gesellschaften dürfen keine derartigen Analysen durchgeführt werden.

Die gesetzlichen Auflagen zum Datenschutz werden bei allen Prüfungshandlungen eingehalten.

Zur Objektivierung können auch logische Abfragen und mathematische Verfahren im Rahmen der digitalen Datenanalyse zum Einsatz kommen. Vor diesem Hintergrund wird zwischen der Unternehmensleitung der Bayer AG und dem Gesamtbetriebsrat Bayer zur Nutzung dieser Analysen folgende freiwillige Gesamtbetriebsvereinbarung getroffen.

4. Einsicht in personenbezogene und personenbeziehbare Datenbestände

Das Verfahren zur Einsicht in personenbezogene und personenbeziehbare Datenbestände ist in einer separaten Gesamtbetriebsvereinbarung mit gleichnamigem Titel geregelt. Die Vorschriften dieser Vereinbarung sind Bestandteil des Prüfungsverfahrens mittels digitaler Datenanalysen.

Ergibt sich aufgrund der Prüfung ein Verdacht auf das Vorliegen einer Straftat, ist eine einzelfall- und personenbezogene Auswertung in Bezug auf die betroffene Person zulässig, auf die sich der Verdacht einer Beteiligung konkret bezieht. Bei Überprüfung des Verdachts finden die konzerninternen Regelungen zur Nutzung elektronischer Kommunikationsmittel und Medien uneingeschränkt Anwendung.

5. Art und Umfang des Zugriffs auf Daten

Zur Vorbereitung der konkreten Prüfungen können alle prüfungsrelevanten Rechnungswesendaten aus den Buchhaltungs- und Verwaltungssystemen auf einen gesicherten Revisionsserver heruntergeladen werden. Dies geschieht in der Praxis nach Vorlage eines schriftlichen Prüfungsauftrages. Zu diesem Zweck wird ein entsprechendes Downloadtool (DAB Exporter) durch die interne Revision eingesetzt, das in Anlage 2 beschrieben ist. Sollte ein anderes Downloadtool eingesetzt werden, ist dies mit der Kommission Neue Technologien und Datenschutz des Gesamtbetriebsrats abzustimmen.

Die Prüfer erhalten die herunter geladenen und qualitätsgesicherten Daten auf verschlüsselten, mobilen Datenträgern. Der mobile Datenträger wird durch ein Passwort geschützt, das dem Datenempfänger bei Übergabe durch eine verschlüsselte Email mitgeteilt wird.

Die interne Revision hat zur Erfüllung ihrer Aufgaben Zugriff auf alle Rechnungswesendaten, wie z. B. auf die produktiven ERP- und BW-Systeme, sowie auf alle Geschäftsunterlagen.

6. Archivierung und Löschung der Prüfungsdaten

Nach Abschluss der Prüfung sind von den Prüfern

- die prüfungsrelevanten Vorgänge und Dokumente mit dem Prüfbericht zu archivieren,
- der mobile Datenträger zur Löschung zurück zu geben und
- die nicht mehr benötigten Datenbestände zu löschen.

Sollten die Daten zur Beweissicherung bei Unregelmäßigkeiten oder Straftaten benötigt werden, erfolgt die Löschung sobald etwaige hieraus resultierende Verfahren abgeschlossen sind bzw. eine Beweissicherung aus rechtlichen Gründen nicht mehr erforderlich ist.

7. Information des Gesamtbetriebsrats

Der Gesamtbetriebsrat wird mindestens einmal jährlich über die Prüfungen, deren Ergebnisse und besondere Vorkommnisse informiert. Hierzu zählt auch die Darstellung der Dokumentation von berichtsrelevanten Informationen.

8. Kündigung / Sonstiges

Diese Gesamtbetriebsvereinbarung tritt zum 01.02.2013 in Kraft. Sie kann mit einer Frist von drei Monaten - erstmals zum 31.12.2013 - gekündigt werden. Im Falle der Kündigung ist die Nachwirkung ausgeschlossen. Die Parteien bekräftigen ihren Willen im Falle der Kündigung dieser Gesamtbetriebsvereinbarung zeitnah Gespräche mit dem Ziel aufzunehmen, eine neue Regelung zu finden.

Sollten eine oder mehrere Bestimmungen dieser Gesamtbetriebsvereinbarung unwirksam sein, bleiben die übrigen in Kraft. Die Parteien verpflichten sich schon jetzt, nach einer Regelung zu suchen, die der unwirksamen am nächsten kommt.

Leverkusen, den 24.01.2013

....

Bayer AG

....

Gesamtbetriebsrat Bayer AG

Anlage 1 zur Gesamtbetriebsvereinbarung „Digitale Datenanalyse“ vom 24.01.2013

Anwendungsvorschriften für den Einsatz von Massendaten

Im Rahmen des Einsatzes von Massendaten auf vom STAAN-Team ausgegebenen mobilen Datenträgern sind folgende Anwendungsvorschriften verbindlich:

1. Bei Daten, die vom STAAN-Team inhaltlich nicht validiert wurden, liegt es im Verantwortungsbereich des Datenempfängers sicherzustellen, dass die angeforderten Tabellen vorhanden sind, vollständig sind (z.B. Archivierungsproblematik) und die gewünschten Vorgaben angewandt wurden.
2. Die übergebenen Daten werden in einer verschlüsselten Datei (Container) auf einem mobilen Datenträger gespeichert. Das Löschen dieser Datei (Container) und die Verwendung des mobilen Datenträgers ohne Verschlüsselung ist nicht gestattet. Des Weiteren darf das Kopieren oder Verschieben der Daten nur auf verschlüsselte CA Notebooks/CA Datenträgern erfolgen, die den allgemeinen Sicherheitsstandards nach der Richtlinie ‚1435 – IT Sicherheit' entsprechen. Es ist zu beachten, dass der Benutzer zur Entschlüsselung des Containers die Software ‚SafeGuard-Private Disk' (Ansprechpartner BBS-IT-Support) benötigt.
3. Soweit die extrahierten Tabellen noch personenbezogene Informationen von Mitarbeitern, wie zum Beispiel User-IDs enthalten, dürfen diese Daten nicht zur Identifizierung der konkreten Personen oder für personenbezogene Auswertungen, Leistungskontrollen etc. verwendet werden.
4. Mobile Datenträger werden vom STAAN-Team ausschließlich für massendatenbezogene Prüfungen ausgegeben und müssen nach dem Abschluss der angegebenen Prüfung (inkl. Nachbereitung) unaufgefordert an das STAAN-Team zurückgegeben werden. Der mobile Datenträger wird durch ein Passwort geschützt, das dem Datenempfänger bei der Übergabe per verschlüsselter E-Mail mitgeteilt wird. Dieses Passwort ist vertraulich und darf nur an Mitarbeiter von BAG CA weitergegeben werden.
5. Bei Dienstreisen sind die länderspezifischen Hinweise im Umgang mit mobilen Datengeräten/-trägern und die länderspezifischen Anforderungen von Corporate Security zu beachten. (s. Intranetseite von Corporate Security).

Sollten eine oder mehrere Bestimmungen dieser Vorschriften mit allgemeinen Bayer Regelungen in Widerspruch stehen, so bleibt die Wirksamkeit dieser Vorschriften im Übrigen hiervon unberührt. Anstelle der unwirksamen Vorschriften treten die gültigen Bestimmungen der Bayer Regelungen.

Hiermit bestätige ich meine Zustimmung zu den oben genannten Anwendungsvorschriften und den Empfang des mobilen Datenträgers.

Name der Festplatte	Ort, Datum
Datenempfänger	Verantwortlicher STAAN

Die Rückgabe des mobilen Datenträger erfolgte am _____. Die gegebenenfalls noch vorhandenen Daten können gelöscht werden.

Datenempfänger	Verantwortlicher STAAN

Anlage 1 zur Gesamtbetriebsvereinbarung „Digitale Datenanalyse" vom 24.01.2013

Prozessbeschreibung: Datendownload und Anonymisierung

Im Rahmen von Audits durch die Revision werden von einem limitierten Mitarbeiterkreis prüfungsbezogen Datendownloads aus SAP® R/3®-Systemen durchgeführt. Zu diesem Zweck wurde eine Schnittstelle auf den betroffenen SAP® R/3®-Systemen eingerichtet. Diese Schnittstellen wurden nur auf den SAP® R/3®-Systemen eingerichtet, die zur Speicherung von Geschäftsdaten verwendet werden. HR-Systeme (z.B. das globale SAP System GHP) sind davon ausgeschlossen. Bei den Daten, die zu Prüfungszwecken heruntergeladen werden, handelt es sich um Geschäftsdaten der Funktionsbereiche Beschaffung, Vertrieb, Materialwirtschaft und Rechnungswesen.

Der Zugriff auf die Tabellen erfolgt mittels des dab:exporters. Der dab:exporter ermöglicht eine GDPdU-konforme Extraktion von SAP® R/3®-Daten (**G**rundsätze zum **D**atenzugriff und zur **P**rüfbarkeit **d**igitaler **U**nterlagen). Der Datenzugriff erfolgt stets im Lesezugriff, so dass eine Änderung von Daten im SAP® R/3®-System ausgeschlossen ist. Die Daten werden auf revisionseigenen externen Festplatten verschlüsselt abgelegt, wobei dem Prüfungsteam das entsprechende Verschlüsselungskennwort mitgeteilt wird.

Bei der Speicherung von Geschäftsdaten (z.B. einer Bestellung, Rechnung, etc.) werden durch die SAP® R/3®-Systeme die User-CWIDs mitgespeichert. Um datenschutzrechtliche Bestimmungen einzuhalten, werden diese während des Downloads und vor der Speicherung auf den Datenträgern von BAG-CA pseudonymisiert, d.h. über einen weiteren Schlüssel, den das Prüfungsteam nicht kennt, verschlüsselt.

Zum Zweck der Pseudonymisierung von personenbezogenen Daten gemäß §32 BDSG wird beim Export von Daten ein Zusatzprogramm verwendet. Bei der Verschlüsselung der Daten wird eine sog. 64 bit DES Verschlüsselungsroutine eingesetzt. Eine automatisierte Entschlüsselung der Usernamen durch BAG-CA ist nicht möglich.

Die Daten werden nach dem Prinzip der Datensparsamkeit den Prüfern zweckgebunden (d.h. prüfungsbezogen) bereitgestellt. Der jeweilige Prüfer verpflichtet sich bei Datenübergabe alle datenschutzrechtlichen Bestimmungen zu beachten. Im Nachgang der Prüfung werden die berichtsrelevanten Daten im Rahmen der gesetzlichen Pflichten auf dem Server der Revision archiviert. Nicht berichtsrelevante Daten werden nach Abschluss der Prüfung gelöscht.